Міністерство освіти і науки України
ДВНЗ «Криворізький національний університет»
Факультет інформаційних технологій
Кафедра комп’ютерних систем та мереж

М Е Т О Д И Ч Н І В К А З І В К И

до виконання лабораторних робіт
з дисципліни **«МЕРЕЖНІ ОПЕРАЦІЙНІ СИСТЕМИ»**
(Windows Server 2016)
для студентів спеціальності
123 «Комп’ютерна інженерія»
усіх форм навчання

Кривий Ріг – 2018

Укладачі: **Кумченко Ю. О.**, канд. техн. наук, ст. викладач
Музика І. О., канд. техн. наук, доцент

Рецензент: **Жосан А. А.**, канд. техн. наук, доцент

Дані методичні вказівки містять завдання та теоретичні відомості для виконання 7-ми лабораторних робіт з вивчення мережної операційної системи Windows Server 2016 з дисципліни «Мережні операційні системи» для студентів спеціальності 123 «Комп'ютерна інженерія».

Детальні теоретичні відомості та приклади використання команд сприятимуть кращому засвоєнню можливостей популярної серверної операційної системи, дозволять самостійно виконати лабораторні роботи.

Розглянуто
на засіданні кафедри
комп'ютерних систем та мереж

Протокол № 7
від 20.02.2018 р.

Схвалено
на вченій раді факультету
інформаційних технологій

Протокол № 7
від 21.02.2018 р.

ЗМІСТ

ВСТУП

Дисципліна «Мережні операційні системи» вивчається студентами спеціальності 123 «Комп'ютерна інженерія» у 7-му семестрі, має обсяг 120 годин (лекції – 18 год., лаб. роботи – 36 год., самостійна робота – 66 год.).

Дисциплінами, що забезпечують курс «Мережні операційні системи» є: «Програмування», «Паралельні та розподілені обчислення», «Архітектура комп'ютерів», «Системне програмування», «Системне програмне забезпечення», «Комп'ютерні мережі», «Комп'ютерні системи».

Метою викладання дисципліни «Мережні операційні системи» є вивчення структури, принципів побудови, концепції та призначення найбільш розповсюджених мережних операційних систем, особливості їх інсталяції, адміністрування, конфігурування та програмування, а також отримання відповідних практичних навичок.

Предметом дисципліни є вивчення основних принципів побудови та знайомство з основними командами операційних систем UNIX, FreeBSD та Windows 2016 Server.

Дані вказівки призначені для вивчення мережної операційної системи Windows Server 2016, які містять 7 лабораторних робіт.

Знання, одержані при вивченні дисципліни «Мережні операційні системи», є необхідними для використання при вирішенні інженерно-технічних задач та фахової діяльності як бакалавра та магістра з комп'ютерної інженерії.

Дисципліна «Мережні операційні системи» викладається одночасно з дисциплінами «Комп'ютерні мережі», «Комп'ютерні системи» та «Захист інформації у комп'ютерних системах» і тісно пов'язана з ними, взаємно забезпечуючи одна одну.

Звіт виконується на папері формату А4, на обкладинці якого вказується тема роботи, прізвище студента та група. Зміст звіту наводиться в кожній лабораторній роботі окремо.

Звіт обов'язково виконується українською мовою охайно, рисунки виконуються з додержанням стандарту ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення».

Лабораторна робота вважається виконаною, якщо студент був присутнім на лабораторних заняттях за розкладом або на додаткових заняттях і консультаціях, успішно виконав програму лабораторних робіт, особисто представив викладачу повністю оформлені звіти з лабораторних робіт згідно з методичними вказівками та завданнями викладача. Лабораторна робота вважається захищеною, якщо студент в усній або письмовій формі відповів на всі запитання викладача стосовно теми роботи та одержав позитивну оцінку.

Знання студентів під час захисту лабораторних робіт оцінюються за наступними критеріями:

а) «відмінно» — якщо студент дає вичерпну відповідь на питання або повністю і вірно виконує практичне завдання;

б) «добре» — якщо студент дає повну відповідь на питання або майже повністю і вірно виконує практичне завдання, при цьому можуть бути такі недоліки: незначні неточності, несуттєві помилки, відсутні вторинні деталі;

в) «задовільно» — якщо студент допустив суттєві помилки при відповіді, виклав не весь матеріал, упустивши значний його об’єм. Відповідь має досить схематичний вигляд, але вірна. При виконанні практичних завдань не досягнута кінцева мета, але хід вирішення правильний.

г) «незадовільно» — якщо не дав відповіді взагалі або дав невірну відповідь. Практичне завдання не виконане і хід вирішення невірний.

Перед виконанням лабораторних робіт група розбивається на бригади, кожна з яких виконує лабораторні роботи згідно свого варіанту. Кількість студентів у бригаді визначається залежно від розміру групи та кількості наявних комп’ютерів у комп’ютерному класі. Кожна бригада створює свій окремий домен, що складається з одного сервера (контролера домена) та одного або двох кліентських вузлів залежно від розміру класу.

ЛАБОРАТОРНА РОБОТА №1

Тема: «Встановлення операційної системи Windows Server 2016. Настроювання служб».

Мета: отримати навички встановлення операційної системи Windows 2016 Server і настроювання мережевих служб ADS (Active Directory Services), DNS (Domain Name Server), DHCP (Dynamic Host Configuration Protocol), побудови Контролеру Домену (Domain Controller).

Теоретичні відомості

Windows Server 2016 — серверна операційна система (ОС) компанії Microsoft. Вона належить до сім'ї операційних систем Windows NT і розбляється паралельно із Windows 10. Перша прев'ю версія (Technical Preview) з'явилася 1 жовтня 2014 року разом із першою прев'ю версією System Cente. Планувалося, що фінальний реліз сервера буде 26 вересня 2016 року, тобто не буде випущена разом з клієнтською операційною системою Windows 10, як було у випадку із останніми трьома випусками операційних систем.

У ***Windows Server 2016*** реалізовані зовсім нові засоби керування системою й адміністрування**.** Ось деякі з них:

- **Active Directory** — розширювана й масштабована служба каталогів, в якій використовується простір імен, заснований на стандартній Інтернет-службі іменування доменів (***Domain Name System, DNS***);
- **IntelliMirror** — засіб конфігурування, що підтримує дзеркальне відображення користувальницьких даних і параметрів середовища, а також центральне адміністрування встановлення та обслуговування програмного забезпечення;
- **Terminal Services** — служби терміналів, що забезпечують віддалений вхід в систему й керування іншими системами ***Windows Server 2016***;
- **Windows Script Host** — сервер сценаріїв Windows для автоматизації таких розповсюджених завдань адміністрування, як створення облікових записів користувачів та звітів у журналах подій.

Хоча в ***Windows Server 2016*** маса інших можливостей, саме ці чотири найбільш важливі для виконання завдань адміністрування. Найбільше це відноситься до ***Active Directory***, тому для успішної роботи системному адміністраторові ***Windows Server 2016*** необхідно чітко розуміти структуру й процедури цієї служби.

При встановленні ***Windows Server 2016*** систему можна конфігурувати як рядовий сервер, контролер домену або ізольований сервер. Розходження між цими типами серверів надзвичайно важливі. Рядові сервери є частиною домена, але не зберігають інформацію каталогу. Контролери домену зберігають дані каталогу й виконують служби аутентифікації та каталогу в рамках домена. Ізольовані сервери не є частиною домена й мають власну БД користувачів, тому ізольований сервер також аутентифікує запити на вхід.

Домени, в яких застосовуються служби ***Active Directory***, називають доменами ***Active Directory***, щоб відрізняти їх від доменів ***Windows NT***. Хоча ***Active Directory*** працює тільки з одним контролером домена, у домені можна й потрібно створити додаткові контролери. Якщо один контролер виходить із ладу, для виконання аутентифікації й інших важливих завдань можна задіяти інші. В домені ***Active Directory*** будь-який рядовий сервер дозволяється підвищити до рівня контролера домену без перевстановлення ОС, як того вимагала ***Windows NT***. Для перетворення рядового сервера в контролер потрібно лише встановити на нього компонент ***Active Directory***. Можлива й зворотня дія: зниження контролера домену до рядового сервера, якщо він не є останнім контролером домену в мережі.

У лабораторній роботі використаємо операційну систему ***Windows Server 2016 Standard Evalutation з вбудованим графічним інтерфейсом***. Ця операційна система має наступні системні вимоги: CPU від 1.4 Ггц (рекомендується 2 Ггц), 2 Гб RAM (рекомендується 4 Гб), 32 Гб місця на диску.

Мережі ***Windows*** структуруються за допомогою служб активного каталогу або ***ADS (Active Directory Services).*** Вони встановлюються й управляються засобами серверів ***Windows 2012/2016***. Усі компоненти комп'ютерної мережі (тобто комп'ютери-користувачі, різноманітні мережні ресурси та ін.) для ***ADS*** є об'єктами, властивості яких визначаються за допомогою різних атрибутів. Всі об'єкти, що входять в ***ADS***, утворюють каталог. Для зручності керування цими об'єктами в ***ADS*** використовуються контейнери, завдання яких полягає в зберіганні інших об'єктів, а також у настроюванні їхньої роботи. Комп'ютери можуть об’єднуватися в логічні одиниці — домени. Кожен домен управляється контролером домену, що зберігає загальну для домену інформацію й виконує загальну централізовану авторизацію користувачів, що приєдналися. На відміну від доменів на базі ***Windows NT***, контролерів у доменах ***Windows 2012/2016*** може бути небагато, і вони рівноправні. Для ще більшого структурування домени можуть поєднуватися в «дерева».

Domain Name Server (сервер доменних імен) — сервер, що містить базу даних з іменами хостів і відповідними їм IP-адресами. Таким чином, користувачі мережі працюють з іменами хостів, а ***DNS*** уже перетворює їх у дійсні IP-адреси.

Контролер домену (Domain controller) — сервер, на якому працюють служби каталогів і розташовується сховище даних каталогу. Контролери домену також відповідають за вхід у мережу й пошук у каталозі. При виборі цієї ролі на сервері будуть встановлені ***DNS*** й ***Active Directory***.

Хід роботи

1. Побудувати мережу з декількох комп'ютерів і зробити один з них сервером. Почнемо з встановлення. Необхідно встановити ***Windows Server 2016 Standard Evalutation***. Встановлення з автозавантажувального CD-диску нічим не відрізняється від встановлення ***Windows 10***. Під час настроювання мови

виберіть ***Ukraine***. Те ж саме виберіть у пункті ***Location*** у тій же закладці. Далі натисніть закладку ***Advanced*** у полі ***Select a language to match the language version of the non-Unicode programs you want to use*** і виберіть ***Russian***. Тим самим забезпечується коректне відображення кирилиці в програмах. Переходимо до наступного пункту.

2. Після встановлення потрібно налаштувати ***Internet Protocol (TCP/IP)***. Переходимо у **Диспетчер серверів** і натискаємо **Налаштувати цей локальний сервер** та шукаємо розділ **wan**. Двічі натискаємо на кнопку ***Properties (Властивості)***, скасовуємо автоматичне одержання IP-адреси, вводимо вручну у поле ***IP address*** адресу сервера згідно варіанту (див. таблицю 1.2), натискаємо ***Tab***, — маска підмережі повинна автоматично заповнитися й прийняти вигляд 255.255.255.0 (всі інші поля повинні залишитися порожніми) (рисунок 1.1).

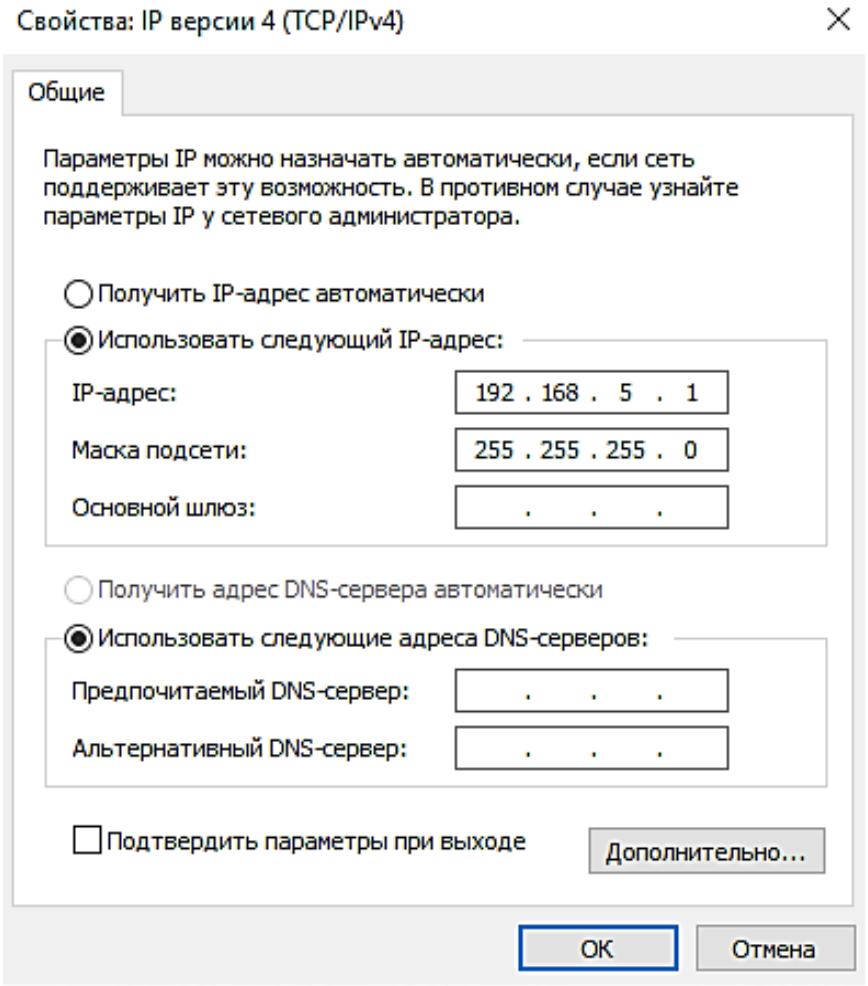

Рисунок 1.1 – Настроювання мережевих параметрів

3. Для спрощення подальшої роботи скористаємося можливістю операційної системи ***Windows 2016 Server*** для адмініструванню сервера, натискаємо ***Пуск (Start)*** → **Диспетчер серверів** (рисунок 1.3).

Додамо нашому серверу домен. Для цього скористаємося вкладкою **“Додати ролі та компоненти ”** та оберемо **“Доменні служби Active Directory”.**

Натискаємо ***New role***, вибираємо ***Custom configuration → Domain Controller (Active Directory) → Domain controller for new domain***. Далі опції: ***Domain in new forest — No, just install and configure DNS on this computer; Full DNS name — ім'я.net*** (рисунок 1.4)*;* вводимо пароль адміністратора (див. таблицю 1.2), перезавантажуємося.

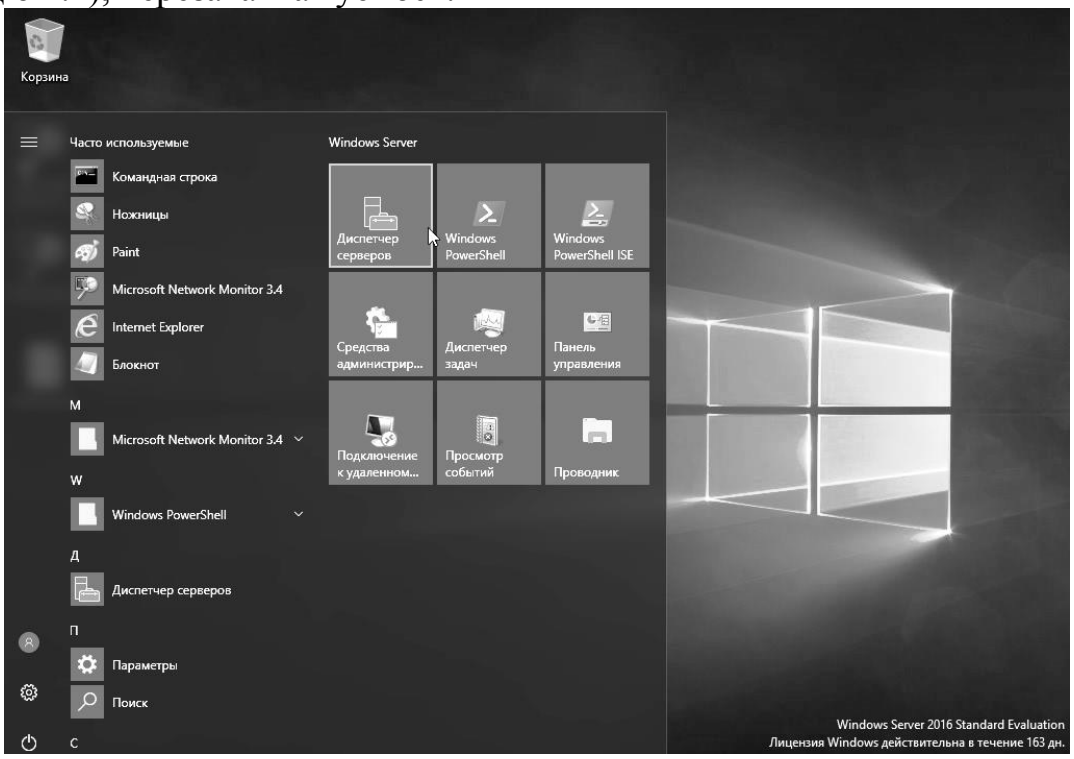

Рисунок 1.2 – Параметри керування сервером

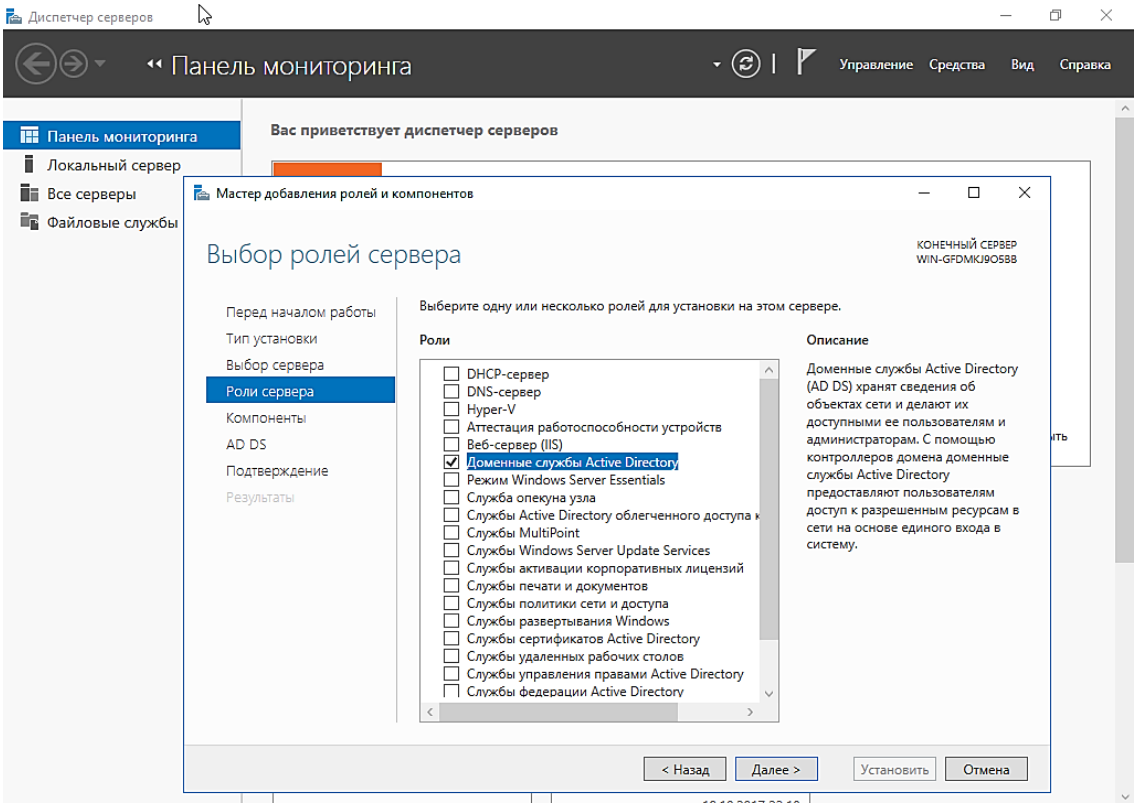

Рисунок 1.3 – Додаваня доменної служби

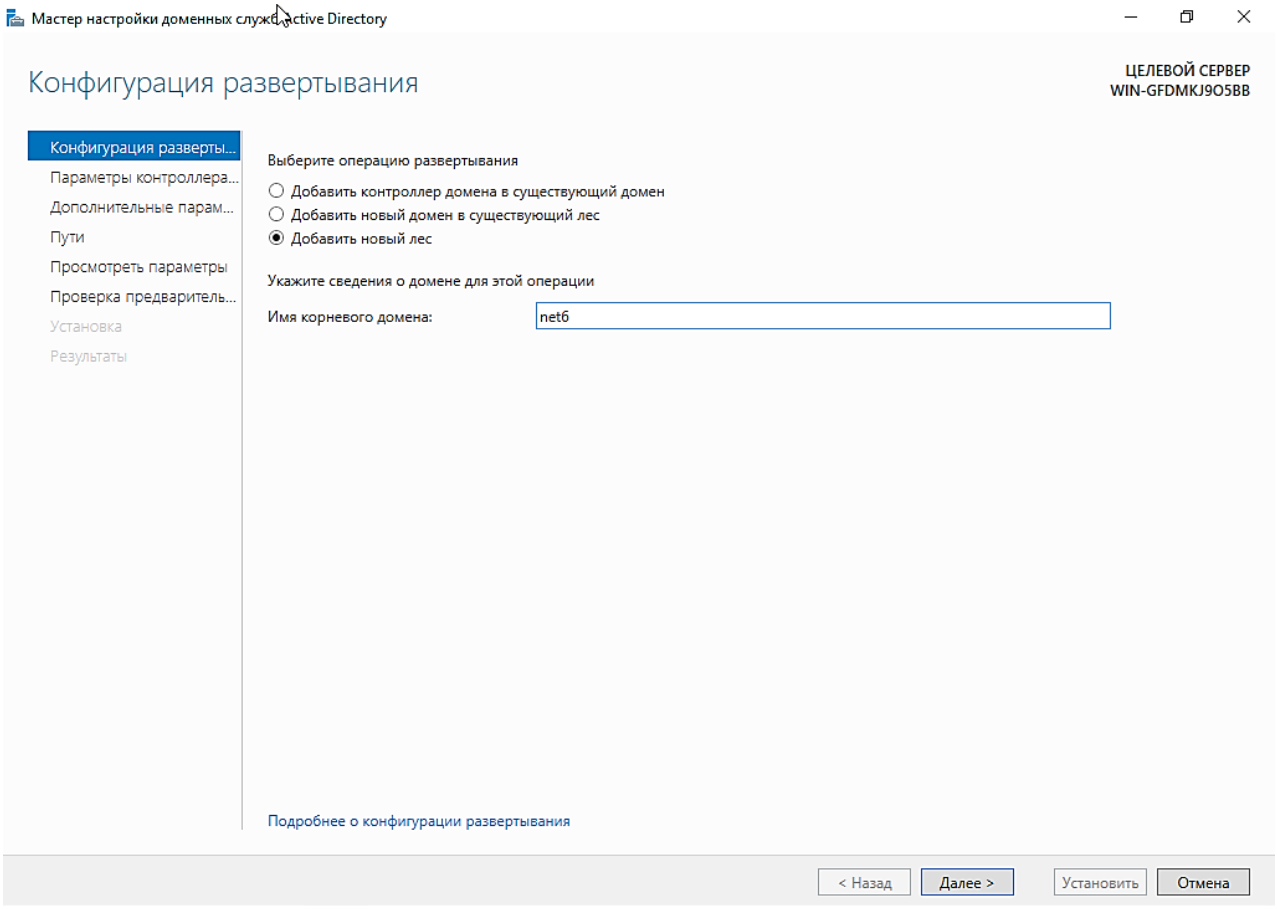

Рисунок 1.4 – Завдання домену імені

Як стало вже зрозумілим, цією послідовністю дій було зроблено сервер ***Контролером Домена (Domain Controller)***, а відповідно, «підняли» на ньому службу ***Active Directory*** й, нарешті, настроїли ***DNS*** на нашому комп'ютері.

4. Для легкості в розширюваності системи необхідно встаноновити й настроїти ***DHCP (Dynamic Host Configuration Protocol*** — протокол динамічної конфігурації хоста). Для цього скористаємося вкладкою **"Додати ролі та компоненти "** та оберемо **"DHCP-сервер"**, у вікні **Диспетчер серверів** обираємо ***Засіб – DHCP - ім'я нашого серверу- IPv4***; Далі натискаємо на ***IPv4*** правою кнопкою миші та обираємо **"Створити область"**(рисунок 1.5)**.** ***Description: ім'я scope***, ***Start IP-Address:*** (див. таблицю 1.2)***; End IP-Address:*** (див. таблицю 1.2); маска підмережі повинна прийняти значення 255.255.255.0, ***Exclusions*** пропускаємо (якщо хочете, можете вказати діапазон тих адрес, області з яких обирати не можна), ***Lease Duration: 8 days*** (період резервування адреси), далі вибираємо ***Yes, I want to configure these options now, Router (Default Gateway)*** — адреса сервера (див. таблицю 1.2) (***Add***), ***Domain Name and DNS servers*** — адреса сервера (див. таблицю 1.2) (***Add***), ***WINS Server.Yes, I want to activate this scope now (Finish)***.

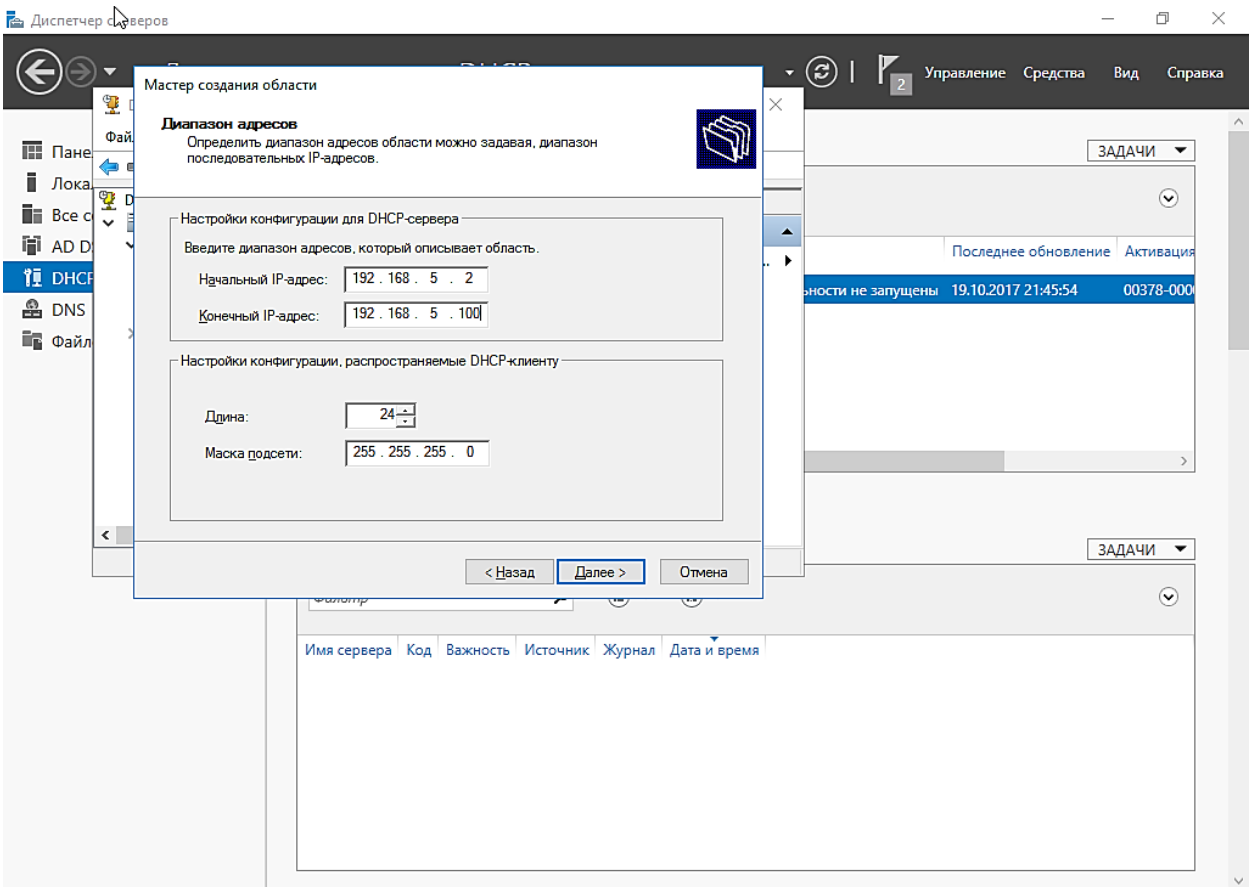

Рисунок 1.5 – Завдання пулу адресів

5. На клієнтському комп'ютері обираємо ***Пуск → Настроювання → Мережа й віддалений доступ до мережі***, двічі клацаємо правою кнопкою миші на ***Підключення до локальної мережі***, обираємо ***Властивості***, потім ***Протокол Інтернету (TCP/IP)***, знову ж ***Властивості***. Обираємо ***Одержати IP-адресу автоматично***.

Далі, натиснувши правою кнопкою миші на іконку ***«Мій комп'ютер»***, обираємо ***Властивості → Мережева ідентифікація → Властивості***. У пункті ***Входить*** вибираємо домен й уводимо обране ***ім'я домена (ім'я.net)*** і натискаємо ***OK***. Виведеться вікно із запитом імені й пароля користувача, що має права для підключення комп'ютера в домен.

Таким чином встановлення операційної системи ***Windows Server 2016*** завершено.

Таблиця 1.1 – Варіанти завдання

№ варіанту	Ім'я домену	IP-адреса сервера	Пароль адміністратора на сервері	Start IP-Address of DHCP Server	End IP-Address of DHCP Server
1	net1	192.168.0.1	net1	192.168.0.2	192.168.0.100
2	net2	192.168.1.1	net2	192.168.1.2	192.168.1.100
3	net3	192.168.2.1	net3	192.168.2.2	192.168.2.100
4	net4	192.168.3.1	net4	192.168.3.2	192.168.3.100
5	net5	192.168.4.1	net5	192.168.4.2	192.168.4.100
6	net6	192.168.5.1	net6	192.168.5.2	192.168.5.100
7	net7	192.168.6.1	net7	192.168.6.2	192.168.6.100
8	net8	192.168.7.1	net8	192.168.7.2	192.168.7.100
9	net9	192.168.8.1	net9	192.168.8.2	192.168.8.100
10	net10	192.168.9.1	net10	192.168.9.2	192.168.9.100

Звіт повинен включати:

1. Тему, мету і порядок роботи.
2. Опис виконання усіх дій.
3. Висновки.

Контрольні питання

1. Які версії ***Windows Server 2016*** вам відомі?
2. Які системні ресурси необхідні для установки ***Windows Server 2016***?
3. Що собою представляє служба ***ADS***?
4. Що таке ***DNS***? Для чого необхідна дана служба?
5. Що собою представляє контролер домену?
6. Які принципово нові служби керування системою й адміністрування були реалізовані в ***Windows Server 2016***?
7. Як можна конфігурувати сервер при встановленні ***Windows Server 2016***?

ЛАБОРАТОРНА РОБОТА №2

Тема: «Настроювання стеку TCP/IP».

Мета: навчитися настроювати IP-адреси, ознайомитися із засобами діагностики підключення TCP/IP, вивчити особливості використання мережевого монітору.

Теоретичні відомості

Transmission Control Protocol/Internet Protocol (TCP/IP) — це промисловий стандарт стека протоколів, розроблений для глобальних мереж. Протокол ***TCP/IP*** був створений в 1970 році для пробної мережі американського міністерства оборони ***ARPANET***, що пізніше розрослася до відомого сьогодні Інтернету. Операційні системи ***UNIX*** використовували протокол ***TCP/IP*** із самого початку. Роль ***TCP/IP*** як основного протоколу мережі Інтернет до сьогоднішнього дня є незаперечним доказом його надійності й функціональності. Іншою його перевагою є наявність версій для будь-яких комп'ютерних платформ.

Операційні системи ***Windows***, починаючи з ***Windows 2000***, уже використовують протокол ***TCP/IP*** як базовий. Це значно прискорює установку нової операційної системи, тому що після завершення установки комп'ютер відразу, без перезавантаження, готовий до роботи в мережі. Однак на відміну від протоколу ***NetBEUI*** протокол ***TCP/IP*** потрібно сконфігурувати. Це можна зробити вже під час встановлення системи або в будь-який інший час. На практиці частіше використовується другий варіант, оскільки під час встановлення не завжди відомі конкретні параметри мережі організації, особливо зовнішнім фахівцям, які звичайне встановлення й виконують. Правильна конфігурація вимагає знання адресації протоколу ***IP***, підмереж, інших служб у мережі, які працюють разом із протоколом ***TCP/IP***, наприклад інструментів для усунення неполадок.

Незаперечною перевагою протоколу ***TCP/IP*** є його можливість до маршрутизації. На практиці це означає, що з його допомогою ви можете звернутися до будь-якої віддаленої мережі (за умови, що з нею існує фізичне з'єднання). Мережа, побудована на протоколі ***TCP/IP***, може зростати без обмежень. Достатнім доказом цьому твердженню є існування мережі Інтернет. Дуже часто про ***TCP/IP*** говорять як про єдиний протокол. Насправді ***TCP/IP*** — це цілий стек протоколів, що складається з декількох рівнів. Для повсякденної роботи адміністратора необов'язково знати ці подробиці. Як приклад протоколів, які є частиною стеку ***TCP/IP***, можна назвати ***ICMP, IGMP, IP, TCP, UDP, HTTP, FTP, SMTP, SNMP, POP3, IMAP4*** або ***NNTP***. Протокол ***TCP/IP*** — це, безумовно, феномен сьогоднішнього дня серед мережних протоколів, і можна рекомендувати для встановлення тільки лише його. Навіть при розгортанні малої мережі доречно із самого початку використати ***TCP/IP***, щоб забезпечити можливість подальшого росту (на який повинна розраховувати кожна організація).

Операційні системи ***Windows***, починаючи з ***Windows 2000***, містять цілий набір утиліт, що слугують для настроювання й налагодження зв'язку за протоколом ***TCP/IP***:

- Утиліта ***IPCONFIG***, що з'явилася в ***Windows NT***, дозволяє переглянути поточні настроювання протоколу ***IP*** і встановлених на даному комп'ютері мережних адаптерів. За допомогою утиліти ***IPCONFIG*** можна тільки переглядати інформацію про IP-адресу, маску підмережі та інші параметри, але не змінювати їх.
- Для перевірки з'єднання між двома вузлами призначена утиліта ***PING***, що теж давно входить до складу ОС ***Windows***. Ця утиліта надсилає на зазначений вузол пакети луни-запиту протоколу ***ICMP*** і рахує отримані від нього пакети луни-відповіді, щоб перевірити, чи доступний цей вузол взагалі та чи надійний зв'язок (яка частка пакетів загубилася). Послідовно тестуючи з'єднання з кожним вузлом, можна виявити місце, в якому зв'язок обірвався. За замовчуванням команда ***PING*** робить 4 спроби надіслати пакет розміром 32 байти. Обидва значення можна змінити за допомогою відповідних ключів: команда ***PING*** без аргументів виводить коротку довідку про припустимі ключі та їхнє призначення.
- Утиліта ***TRACERT*** використовується для відстеження маршруту пакету, надісланого поточним хостом віддаленному. Вона може здатися більш зручною й змістовною, ніж ***PING***, особливо в тих випадках, коли віддалений хост недосяжний. Також можна визначити район проблем зі зв'язком стосовно, наскільки далеко буде відслідковано маршрут. Якщо побачите рядок із зірочками (*****) або з повідомленнями типу ***"Destination net unreachable" , "Destination host unreachable"*** або ***"Request time out"***, можливо, це означає, що виявлено район проблеми зі зв'язком.

У ***TCP/IP*** може використовуватися особливий спосіб призначення адрес — ***APIPA***. При відсутності сервера ***DHCP*** комп'ютер під керуванням ***Windows,*** настроєний на використання ***DHCP***, може призначити собі ***IP***-адресу автоматично. Наприклад, це може відбутися, якщо в мережі немає сервера ***DHCP*** або якщо сервер ***DHCP*** тимчасово відключений для обслуговування. Для автоматично призначуваних IP-адрес агентством ***IANA (Internet Assigned Numbers Authority)*** зарезервований діапазон адрес 169.254.0.0-169.254.255.255.

Отже, адреса, надана ***APIPA***, не буде конфліктувати з іншими адресами. Після призначення ***IP***-адреси для мережного адаптера комп'ютер може використати протокол ***TCP/IP*** для зв'язку з будь-яким іншим комп'ютером у даній локальній мережі, що настроєний для використання ***APIPA*** або що має вручну встановлену ***IP***-адресу, що належить до діапазону адрес 169.254.X.Y (де X.Y — унікальний ідентифікатор клієнта) з маскою підмережі 255.255.0.0.

Варто мати на увазі, що комп'ютер не може зв'язуватися з комп'ютерами в інший підмережі або з комп'ютерами, що не використовують функцію автоматичного призначення ***IP***-адреси. За умовчуванням функція автоматичного призначення ***IP***-адреси активована. Може знадобитися її відключення в наступних випадках:

- у мережі використовуються маршрутизатори;
- мережа підключена до Інтернету без ***NAT*** або проксі-серверу.

При перемиканні між ***DHCP*** й автоматичним призначенням IP-адрес з'являються повідомлення ***DHCP*** (якщо вони не відключені). Якщо повідомлення ***DHCP*** були відключені, то для повторного включення варто змінити значення параметра реєстру PopupFlag у наступному розділі реєстру з 00 на 01:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Vx\DHCP

Щоб зміни набули чинності, необхідно перезавантажити комп'ютер.

Щоб визначити, чи використає ***APIPA*** комп'ютер під керуванням ***Windows Server 2016***, уведіть у командний рядок команду ***IPconfig***. Якщо в полі ***«Автонастройка включена»*** зазначено ***«Так»,*** а поле ***«IP-адреса автонастройки»*** містить адреса 169.254.x.y (де x.y — унікальний ідентифікатор клієнта), комп'ютер використає ***APIPA***. Якщо в поле ***«Автонастройка включена»*** зазначено ***«Ні»***, комп'ютер у цей момент не використає ***APIPA***.

Для відключення автоматичного призначення ***IP***-адреси існує кілька методів.

Можна настроїти ***TCP/IP*** вручну, при цьому буде також відключений ***DHCP***. Можна внести зміни до системного реєстру для відключення функції автоматичного призначення ***IP***-адреси (але не ***DHCP***).

Хід роботи

1. Запустіть команду ***ipconfig***. Поточною адресою повинна бути ***IP***-адреса автонастроювання типу 169.254.X.Y. Ця адреса була призначена за допомогою ***APIPA***.
2. Призначте статичну адресу комп'ютеру (див. таблицю 2.1).
3. Настройте комп'ютер на автоматичне одержання адреси за допомогою ***DHCP***-сервера (див. таблицю 2.1). На вкладці альтернативної конфігурації задайте адресу.

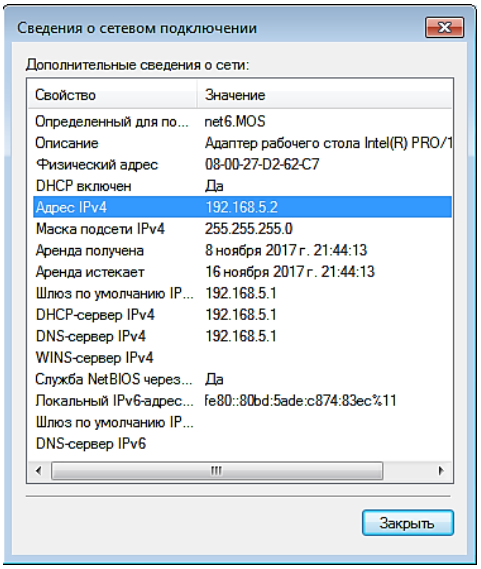

Рисунок 2.1 – Отримання клієнтом IP з заданого пулу адресів

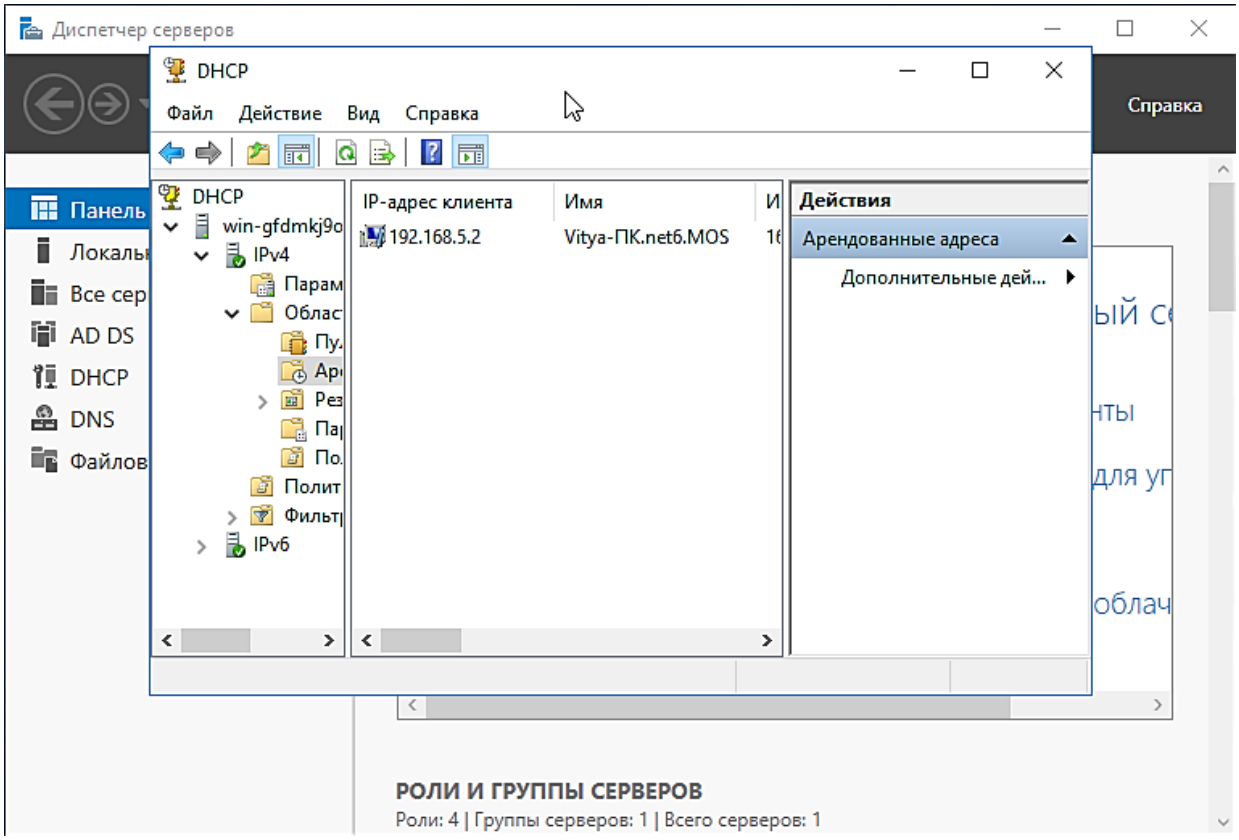

Рисунок 2.2 – Автоматичне додавання IP адреси до арендованих на сервері

4. Знову виконайте ***ipconfig*** і проаналізуйте результати.
5. Запустіть команду ***ping***. Перевірте зв'язок із сусіднім комп'ютером своєї мережі з її допомогою. Спробуйте звернутися до нього як за адресою, так і за іменем.
6. Перевірте зв'язок із комп'ютером наступної за номером бригади за допомогою команди ***ping***. Спробуйте звернутися до нього як за адресою, так і за іменем.
7. Скористайтеся утилітою ***Microsoft Network Monitor 3.4.***(завантажте її з офіційного сайту Microsoft).
8. Відкрийте ***Microsoft Network Monitor 3.4*** і виберіть мережу, в якій перебуває сусідній комп'ютер. Натисніть кнопку ***Почати запис даних (Start)***. Виконайте команду ***ping <Сусідній комп'ютер>***. Натисніть кнопку ***Закінчити запис і переглянути дані (Stop)***. Проаналізуйте отримані дані. Збережіть ці дані у файлі ***PingCapture.cap*** (рисунок 2.3)**.**
9. Відкрийте ***PingCapture.cap.*** У панелі ***Сводка*** виберіть будь-який кадр із протоколом ***ICMP***. Скопіюйте його в буфер обміну ***(Ctrl+C)***. Вставте текст, наприклад, у Блокнот. Збережіть цей текст у файлі ***ICMP.frame.***

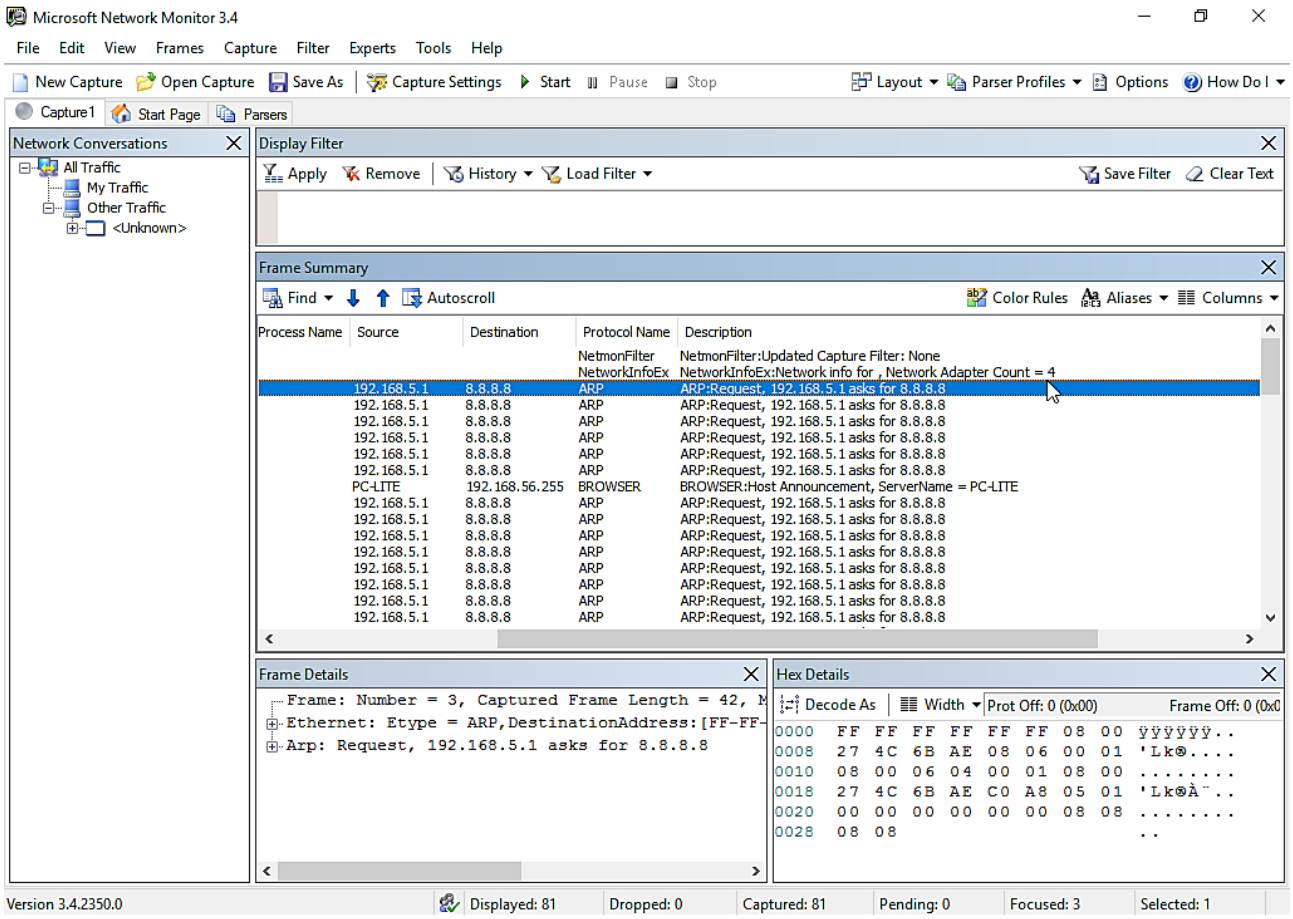

Рисунок 2.3 – Головне вікно Microsoft Network Monitor 3.4

10. Запустіть службу ***Telnet*** (за замовчуванням вона відключена з міркувань безпеки). Підключиться до сусіднього комп'ютера своєї мережі командою ***telnet <сусідній комп'ютер>***. Після проходження аутентифікації з'явиться командний рядок віддаленого комп'ютера. Виконайте команду ***netdiag***. Проаналізуйте результати. Збережіть у файлі звіт про діагностику мережі командою ***netdiag > NetdiagOutput.txt.*** Збережіть у файлі докладний звіт про діагностику мережі командою ***netdiag /v > VerboseNetdiagOutput.txt.*** Порівняйте інформацію у файлах ***NetdiagOutput.txt***, ***VerboseNetdiag Output.txt*** й у раніше створеному ***HTML***-файлі. Не забудьте відключити службу ***Telnet***.

Таблиця 2.1 – Варіанти завдання

№ варіанту	Статична IP-адреса клієнтського вузла	IP-адреса сервера	Start IP-Address of DHCP Server	End IP-Address of DHCP Server
1	192.168.0.101	192.168.0.1	192.168.0.2	192.168.0.100
2	192.168.1.101	192.168.1.1	192.168.1.2	192.168.1.100
3	192.168.2.101	192.168.2.1	192.168.2.2	192.168.2.100
4	192.168.3.101	192.168.3.1	192.168.3.2	192.168.3.100
5	192.168.4.101	192.168.4.1	192.168.4.2	192.168.4.100
6	192.168.5.101	192.168.5.1	192.168.5.2	192.168.5.100
7	192.168.6.101	192.168.6.1	192.168.6.2	192.168.6.100
8	192.168.7.101	192.168.7.1	192.168.7.2	192.168.7.100
9	192.168.8.101	192.168.8.1	192.168.8.2	192.168.8.100
10	192.168.9.101	192.168.9.1	192.168.9.2	192.168.9.100

Звіт повинен включати:

1. Тему, мету і порядок роботи.
2. Опис виконання усіх дій.
3. Висновки.

Контрольні питання:

1. Як працює ***APIPA*** спосіб призначення адрес? Які дії можна виконати за допомогою ***ipconfig***?
2. Що таке адреса шлюзу й адреси ***DNS***-серверів?
3. У якому випадку буде призначена альтернативна адреса?
4. Яка інформація відображається в панелі ***Сводка***, ***Відомості***, ***Шістнадцятковий***?
5. Які відмінності між поданням кадру в панелях ***Мережевого монітора*** й у вигляді текстового фрагмента?
6. Які призначення утиліт ***PathPing***, ***Tracert***, ***Ping*** і способи їхнього застосування?
7. У яких ситуаціях ***PathPing*** переважніше ***Tracert***?
8. Що собою представляє служба ***Telnet***?

ЛАБОРАТОРНА РОБОТА №3

Тема: «Керування обліковими записами користувачів в Windows Server 2016».
Мета: набуття навичок керування обліковими записами користувачів, а також їхніми профілями.

Теоретичні відомості

Умовою роботи будь-якої мережі, звичайно ж, є наявність у ній користувачів й комп'ютерів. Щоб користувач взагалі міг почати роботу на робочій станції, йому повинна бути дозволена реєстрація на ній. Крім того, потрібно, щоб кожному користувачеві було забезпечено хоча б невеликий ступінь свободи, тобто щоб кожний з них міг відрегулювати свій робочий простір відповідно до власних потреб, не порушуючи при цьому загальних принципів мережі. Важливо також, щоб він мав виняткове право доступу до своїх документів. Виходячи із цього, не слід дозволяти всім користувачам реєструватися під одним й тим же обліковим записом і тим більше не варто надавати їм права користувача ***«Адміністратор»***. Тобто для кожного користувача потрібно створити власний обліковий запис.

При створенні нового користувача можна задавати наступні параметри:

- ***Вимагати зміну пароля при наступному вході в систему (User Must Change Password At Next Logon)*** — встановлено за замовчуванням. Дуже зручний засіб для того, щоб пароль користувача знав тільки він. Ви створюєте обліковий запис, наприклад, зі стандартним паролем ***Microsoft (p@s$w0rd)*** і вимагаєте, щоб користувач змінив його відразу ж при запуску системи. Користувач просто не ввійде в систему, не змінивши пароль.
- ***Заборонити зміну пароля користувача (User Cannot Change Password)*** — встановіть цей прапорець, якщо цим обліковим записом користуються декілька користувачів у домені (в тому числі, це стосується облікового запису ***Гість (Guest)***, адже якщо якийсь користувач випадково змінить пароль, то доступ до системи буде неможливий для інших користувачів, що використовують обліковий запис.
- ***Термін дії пароля необмежений (Password Never Expires)*** — використовуйте цей прапор для не дуже захищених мереж (типу домашньої). У захищених мережах його обов'язково треба знімати, тому що паролі користувачів, що мають доступ до конфіденційної інформації, повинні змінюватися регулярно.
- ***Відключити обліковий запис (Account is disabled)*** — для створення користувачів, яким поки непотрібно входити в мережу.

Після створення користувача можна переглянути відомості про нього. Певні властивості були вже настроєні при створенні користувача. Розглянемо призначення деяких з них:

- ***Час входу (Logon Hours)*** — дозволяє настроїти час, коли користувачеві дозволено входити в мережу.

- ***Вхід на (Log On To)*** — визначення комп'ютерів, з яких користувачеві дозволено входити в домен.
- ***Зберігати пароль, використовуючи зворотнє шифрування (Store Password Using Reversible Encryption)*** — цей параметр дозволяє зберігати пароль в ***Active Directory*** без використання потужного алгоритму для шифрування хешируванням (між іншим — без можливості зворотнього перетворення). Використовується для підтримки додатків, яким потрібно знати пароль користувача. Користуйтеся цим параметром тільки у випадку гострої потреби, тому що це істотно послабляє безпеку (паролі, які зберігаються з використанням звортнього шифрування, для досвідченого хакера практично те ж саме, що й пароль, записаний у блокноті відкритим текстом).
- ***Термін дії облікового запису (Account Expires)*** — дозволяє задати дату закінчення дії облікового запису.

Робочу групу, також називають мережею ***peer-to-peer*** або ***одноранговою мережею рівноправних користувачів***, відрізняють наступні основні характеристики:

- ***Робоча група*** — це просте й дешеве рішення завдання об'єднання в мережу невеликої кількості користувачів.
- У мережі типу «робоча група» всі вузли рівноправні й перебувають на тому самому рівні. Вузли не мають можливості ефективно співпрацювати, і не існує простого способу їх одноманітно адмініструвати.
- Кожен користувач повинен мати обліковий запис на кожному з комп'ютерів, за якими йому потрібно працювати.
- Облікові записи користувачів зберігаються на локальному комп'ютері в базі даних системи безпеки ***(SAM, Security Account Manager)***.
- Щоб працювати з ресурсами віддаленого комп'ютера, користувачі повинні мати на ньому обліковий запис із тимож реєстраційним іменем і паролем, що й на локальному комп'ютері. У противному випадку при кожному звертанні до мережевого ресурсу йому доведеться заново вводити ім'я і пароль.
- Якщо користувач захоче змінити пароль, він повинен буде зробити це на всіх вузлах, де в нього є обліковий запис. Якщо він цього не зробить, він втратить прямий доступ до поділюваних ресурсів, розташованих на інших вузлах.
- Будь-які настроювання безпеки, виконані з консолі Локальні параметри безпеки, дійсні тільки на локальному комп'ютері.

Робоча група — це структура, призначена для малих мереж (до десятка комп'ютерів), коли користувачі поєднуються для того, щоб мати доступ до мережних ресурсів, таких як поділювані папки або мережні принтери. Може здатися, що така структура неефективна, але в неї є певні переваги. Робочу групу легко адмініструвати, і впоратися з нею може адміністратор мінімальної кваліфікації.

Хід роботи

1. Для керування сервером скористаємося консоллю mmc. Натисніть **Пуск\Виконати... (Start\Run...)**, у текстовому полі введіть **mmc** і натисніть **[Enter].** Відкриється вікно (рисунок 3.1) з назвою **«Консоль1»(«Console1»).** Натискаємо **Файл\Додати або видалити оснащення (File\Add/Remove Snap-In)**, далі вибираємо **Додати (Add)** і зі списку запропонованих інструментів додаємо в список тільки необхідні (рисунок 3.2). Це робиться шляхом натискання на кнопку **Додати (Add)**. Натисніть **Закрити\ОК (Close\Ok)** — і одержите кілька відкритих елементів керування в одному вікні. Далі консоль можна зберегти й відкривати вже настроєну. Таким чином, всі необхідні інструменти будуть завжди перебувати під рукою. Перш ніж ми перейдемо до створення користувачів нашого домену, необхідно виконати кілька попередніх дій. По-перше, необхідно визначити, де будуть зберігатися профілі користувачів. Нехай у нас це буде папка **User profiles** на диску D. Після створення цієї папки необхідно відкрити до неї загальний доступ (рисунок 3.3) і дати дозвіл усім на читання та зміну.

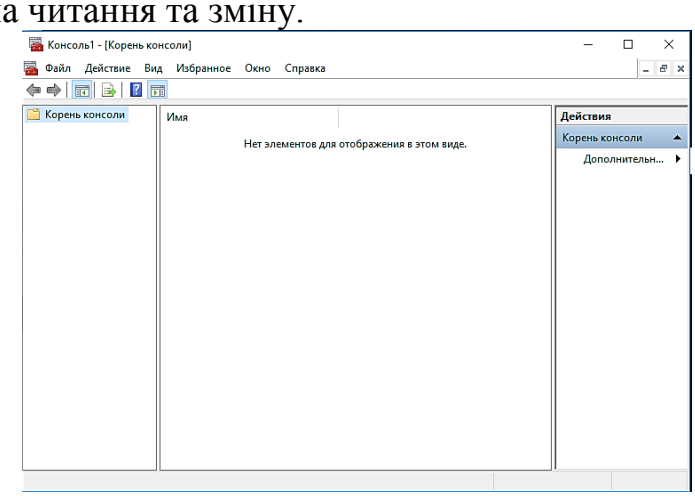

Рисунок 3.1 – Вікно консолі

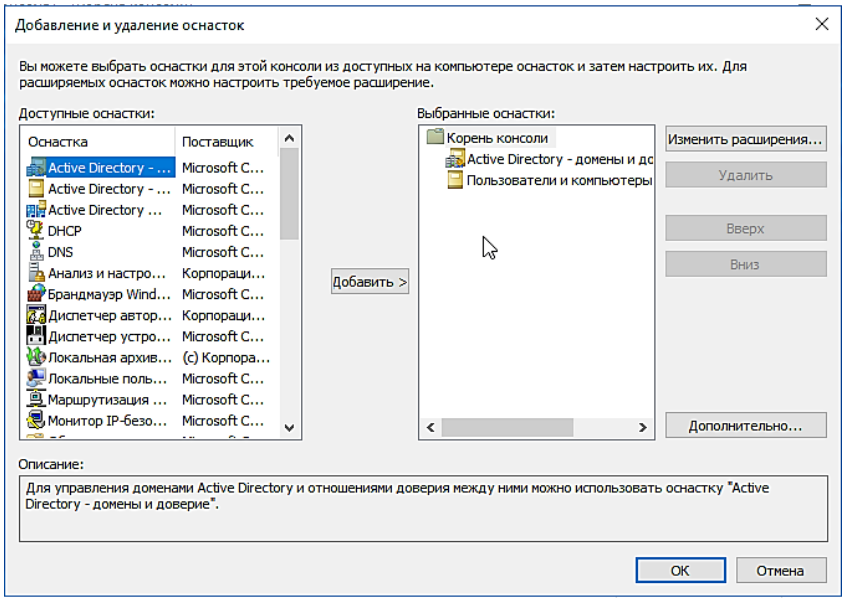

Рисунок 3.2 – Додавання оснасток

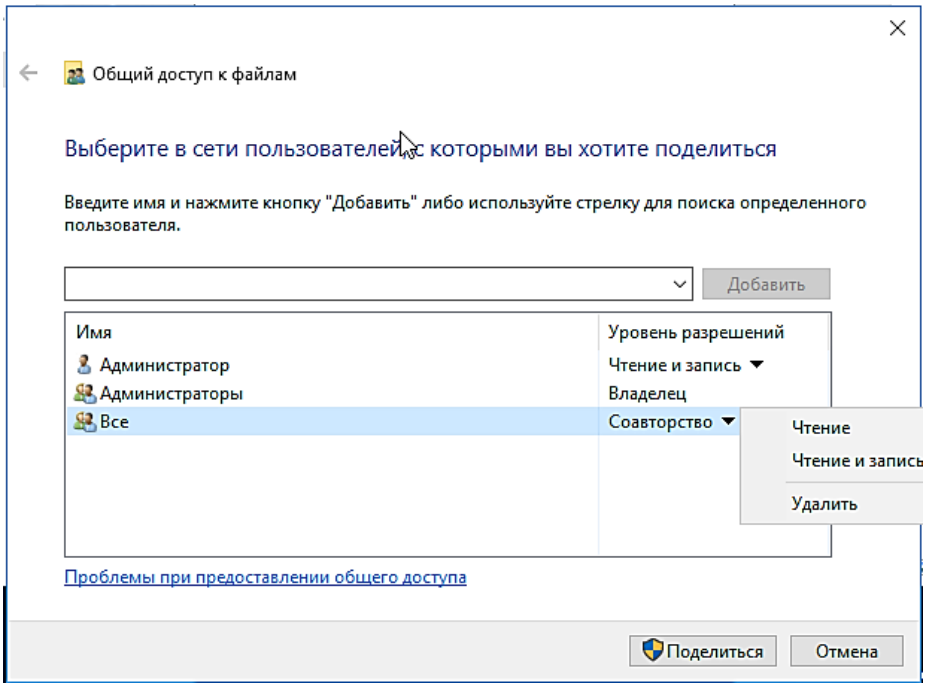

Рисунок 3.3 – Відкриття загального доступу

2. Створимо першого користувача (один з членів вашої бригади) й помістимо його не в стандартному контейнері **Users**, а в контейнері **MyUnit\Users.** Натискаємо правою кнопкою миші на назві домена в оснащенні «Active Directory Users and Computers», вибираємо **Створити\ Підрозділ (New\OrganisationUnit)**, вводимо назву контейнера й натискаємо **ОК**(рисунок 3.4). Такимож чином створюємо ще два контейнери у вже створеному: **Users** й **Computers**. Тепер, вибравши потрібний нам контейнер **(MyUnit\Users)**, вибираємо в меню **Дія (Action)** пункт **Створити\Користувач (New\User)**, створюємо нового користувача (ці дії еквівалентні натисканню правої кнопки миші на контейнері й вибору пункту **Створити\Користувач(New\ User)**). Відкриється діалогове вікно **«Новий об'єкт – Користувач» (New Object – User)**. На його першій сторінці буде необхідно ввести відомості про ім'я користувача (рисунок 3.5).

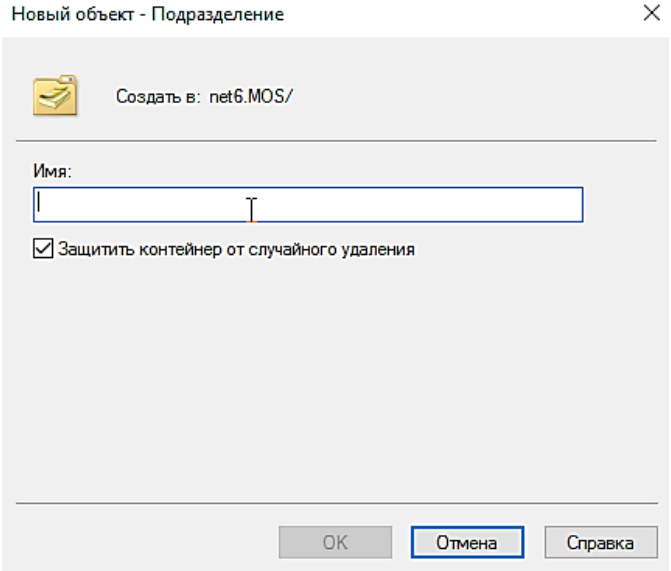

Рисунок 3.4 – Створення контейнеру

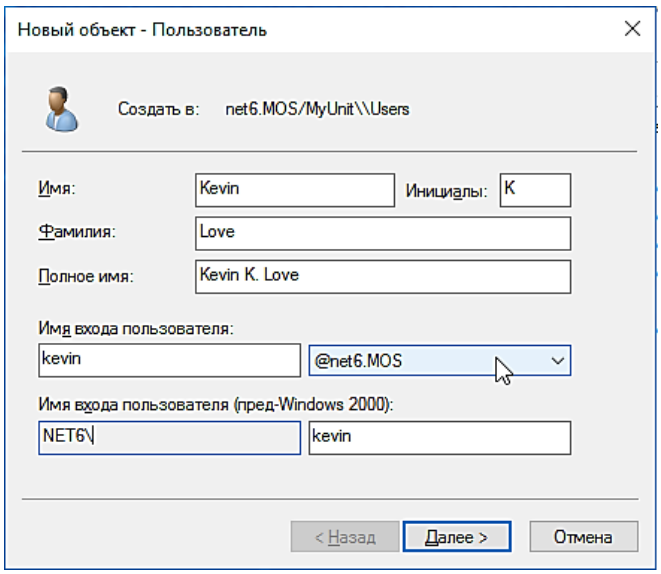

Рисунок 3.5 – Введення відомостей про нового користувача

3. Закінчивши введення цих значень натискаємо **Далі (Next)**. Бачимо другу сторінку, на якій треба буде ввести пароль користувача, а також встановити керуючі прапорці цього облікового запису. Зробіть так, щоб новий користувач не міг увійти в систему доти, доки не змінить пароль, що ви ввели. Встановивши необхідні параметри, натискаємо кнопку **Далі\Готово (Next\Finish)**, закінчуємо створення нового користувача в каталозі **Active Directory**(рисунок 3.6).

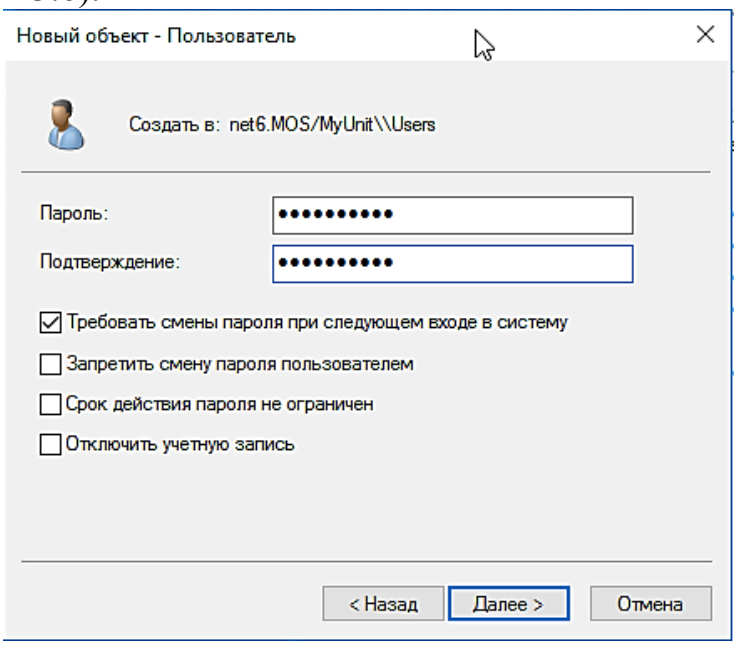

Рисунок 3.6 – Введення паролю нового користувача

4. Перегляньте відомості про нових користувачів. Для цього вибираємо в меню **Дія (Action)** пункт **Властивості (Properties)**. Далі відкриється діалогове вікно, в якому перебуває весь спектр інформації про цього користувача. Особливу увагу зверніть на закладку **Обліковий запис (Account)** (рисунок 3.7).

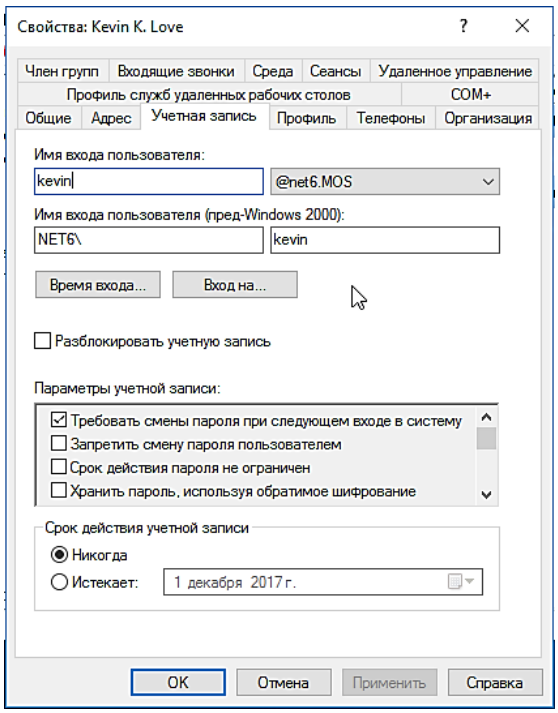

Рисунок 3.7 – Вікно відомостей про користувача

5. Аналогічним чином створіть облікові записи для всіх інших членів вашої бригади з різними налаштуваннями. Порівняйте відомості, які відображаються у вікні відомостей користувача. Зробіть властивості для всіх користувачів однаковими одночасно.
6. Переглянете відомості про користувачів за допомогою команди **net user**.
7. Обмежте термін дії одного з користувачів згідно **таблиці 3.1** (рисунок 3.8).

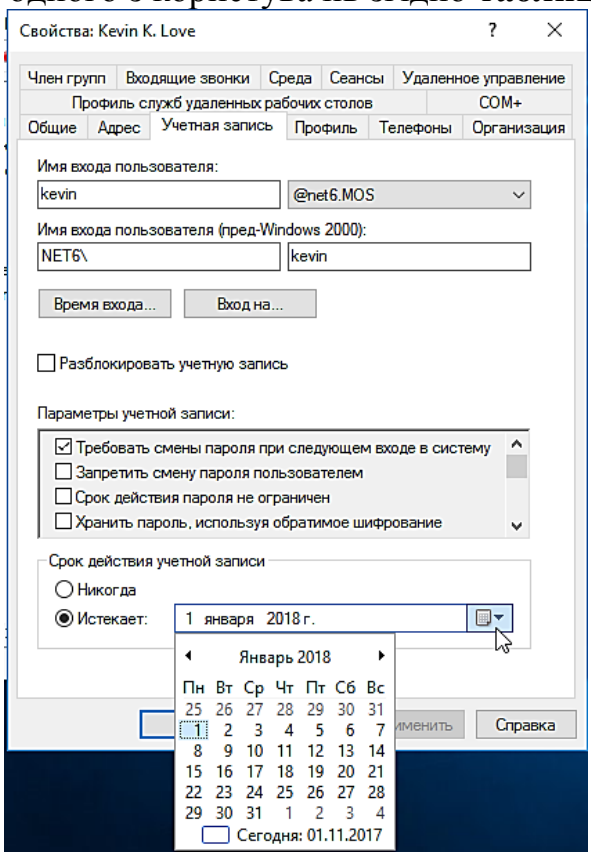

Рисунок 3.8 – Обмеження терміну дії користувача

8. Поставте обмеження за годинами доступу до мережі **(див. таблицю 3.1)** (рисунок 3.9).

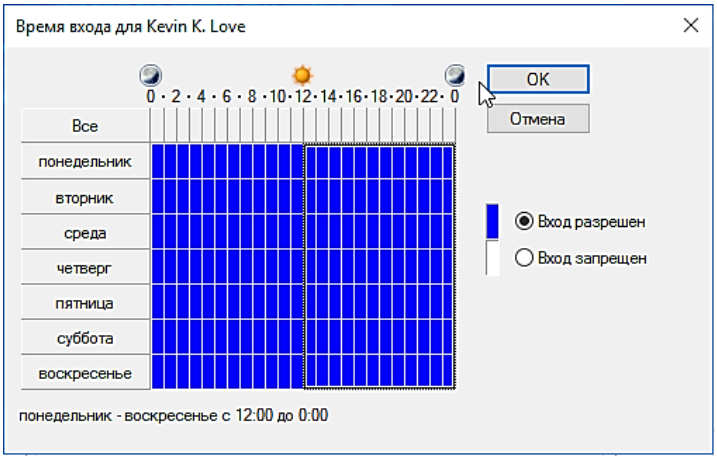

Рисунок 3.9 – Обмеження за годинами доступу до мережі користувача

9. Створіть групу користувачів мережі (див. таблицю 3.1). Для цього виберіть контейнер, клацніть правою кнопкою миші й виберіть пункт **Створити\ Група (New\Group)**. Потім задайте тип й область дії створюваної групи.

Таблиця 3.1 – Варіанти завдання

№ варіанту	Ім’я домену	Обмеження терміну дії облікового запису	Обмеження за годинами доступу до мережі	Назва групи
1	net1	тиждень	з 9 до 17	net1
2	net2	2 тижні	з 7 до 18	net2
3	net3	3 тижні	з 20 до 8	net3
4	net4	4 тижні	з 8 до 16	net4
5	net5	місяць	з 16 до 20	net5
6	net6	2 місяці	з 12 до 24	net6
7	net7	3 місяці	з 8 до 20	net7
8	net8	4 місяці	з 16 до 8	net8
9	net9	5 місяці	з 11 до 19	net9
10	net10	пів року	з 10 до 19	net10

Звіт повинен включати:

1. Тему, мету і порядок роботи.
2. Опис виконання усіх дій.
3. Висновки.

Контрольні питання:

1. Як створити користувача?
2. У якому каталозі зберігаються відомості про користувача?
3. Яка команда дозволяє переглядати відомості про користувачів?
4. Як можна задати тимчасове обмеження для користувача?
5. Чи може користувач поміняти пароль для доступу в мережу без відома адміністратора?
6. Що собою представляє робоча група?
7. У чому відмінність робочої групи від домену?

ЛАБОРАТОРНА РОБОТА №4

Тема: «Розгортання DNS-серверу, конфігурування DHCP-серверів та клієнтів».
Мета: вивчити особливості завдання імен комп'ютерів, архітектуру DNS, настроювання DNS-сервера, особливості рекурсивних запитів, використання та настроювань DHCP-серверів і клієнтів.

Теоретичні відомості

DNS (англ. Domain Name System — система доменних імен) — розподілена система перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в ***IP***-адресу. ***DNS*** працює в мережах ***TCP/IP***. Інколи ***DNS*** може зберігати й обробляти й зворотні запити, визначення імені хоста за його ***IP*** (***PTR***-запису).

На зорі становлення Інтернету (коли він ще був ARPANET'ом) проблема перетворення імені хоста (комп'ютера або іншого мережевого пристрою) в ***IP***-адресу вирішувалася веденням довгих списків, що включали всі комп'ютери мережі, причому копія такого списку повинна була бути присутньою на кожному комп'ютері. Зрозуміло, що зі зростанням мережі ця технологія перестала задовольняти — адже ці файли треба було ще й синхронізувати, не кажучи вже про їхній розмір. Деякі «пережитки» цього підходу можна виявити й зараз: існує файл ***HOSTS*** (і в ***UNIX***, і в ***Windows***), в якому можна прописувати адреси серверів, з якими регулярно працюєте (до речі, саме його використання лежить в основі багатьох «прискорювачів Інтернету» — такі програми просто записують адреси серверів, до яких ви звертаєтеся, у файл ***HOSTS*** і при наступному зверненні беруть дані з нього, не витрачаючи час на запит до ***DNS***-сервера).

На зміну «однофайловій» схемі прийшла ***DNS*** — ієрархічна структура імен. Існує ***«корінь дерева»*** з іменем ***"."*** (крапка). Оскільки корінь єдиний для всіх доменів, то крапка наприкінці імені звичайно не ставиться (але вона використовується в описах ***DNS***). Нижче кореня лежать домени першого рівня. Їх небагато — ***com, net, edu, org, mil, int, biz, info, gov*** і т.д. і домени держав, наприклад, ***ua, ru***. Ще нижче перебувають домени другого рівня, наприклад, ***listsoft.ru***. Ще нижче — третього й т.д.

DNS-сервер працює як гарний комп’ютерник: він завжди або знає відповідь, або знає в кого запитати. Ієрархічність ***DNS***-серверів — річ досить цікава, якщо простежити проходження запиту. При встановленні (точніше, при настроюванні) клієнтові вказується як мінімум один ***DNS***-сервер (як правило, їх два) — його адреса призначається провайдером. Клієнт надсилає запит цьому серверу. Сервер, одержавши запит, або відповідає сам (якщо відповідь йому відома), або пересилає запит на вищій в ієрархії сервер (якщо він відомий) або на кореневий (кожному ***DNS***-серверу відомі адреси кореневих ***DNS***-серверів). Так виглядає «вертикальна ієрархія». Потім запит починає спускатися вниз — кореневий сервер пересилає запит серверу першого рівня, той — серверу другого рівня й т.д.

Крім «вертикальних» зв'язків, у серверів є ще й «горизонтальні» відносини — "первинний — вторинний". Дійсно, якщо припустити, що сервер, що обслуговує якийсь домен і працює «без страховки» раптом перестане бути доступним, то всі машини, розташовані в цьому домені, виявляться недоступними. Саме тому при реєстрації домена другого рівня висувається вимога вказати мінімум два сервери ***DNS***, які будуть цей домен обслуговувати.

DNS-сервери бувають рекурсивні й нерекурсивні. Перші завжди повертають клієнтові відповідь — вони самостійно відслідковують відсилання до інших ***DNS***-серверів й опитують їх. Нерекурсивні сервери повертають клієнтові його запити, і клієнт повинен самостійно опитувати зазначений сервер. Рекурсивні сервери зручно використовувати на низьких рівнях, зокрема, у локальних мережах. Справа в тому, що вони кешують всі проміжні відповіді, і при наступних запитах відповіді будуть повертатися набагато швидше. Нерекурсивні сервери звичайно знаходяться на верхніх щаблях ієрархії — оскільки вони одержують дуже багато запитів, то для кешування відповідей ніяких ресурсів не вистачить.

Корисною властивістю ***DNS*** є вміння використовувати «пересилання» (***forwarders***). Це прискорює дозвіл імен. «Чесний» ***DNS***-сервер самостійно опитує інші сервери й знаходить потрібну відповідь, але якщо ваша мережа підключена до Інтернету через повільну лінію (наприклад, ***dial-up***), то цей процес може займати досить багато часу. Замість цього можна перенаправляти всі запити, скажімо, на сервер провайдера, а потім приймати його відповідь. Використання «пересилювачів» може виявитися цікавим і для великих компаній з декількома мережами: у кожній мережі можна поставити відносно слабкий ***DNS***-сервер, вказавши в якості «пересилювача» більш потужну машину, підключену через швидку лінію. При цьому всі відповіді будуть кешуватися на цьому потужному сервері, що прискорить дозвіл імен для всієї мережі.

Для кожного домена адміністратор веде базу даних ***DNS***. Ця база даних представляє собою набір простих текстових файлів, розташованих на основному (первинному) сервері ***DNS*** (вторинні сервери періодично копіюють до себе ці файли). У файлах конфігурації сервера вказується, в якому саме файлі знаходяться описи яких зон, і чи є сервер первинним або вторинним для цієї зони.

Елементи бази ***DNS*** часто називають ***RR*** (скорочення від ***Resource Record***). Базовий формат запису виглядає так:

[ім'я] [час] [клас] тип дані

Ім'я може бути відносним або абсолютним ***(FQDN — Fully Qualified Domain Name)***. Якщо ім'я відносне (не закінчується крапкою), то до нього автоматично додається ім'я поточного домену. Наприклад, якщо в домені ***listsoft.ru*** описується ім'я ***«www»***, то повне ім'я буде інтерпретуватися як ***"www.listsoft.ru."*** Якщо ж це ім'я вказати як ***"www.listsoft.ru"*** (без останньої крапки), то воно буде вважатися відносним і буде інтерпретовано як ***"www.listsoft.ru.listsoft.ru."***

Час задає інтервал часу в секундах, протягом якого дані можуть зберігатися в кеші сервера.

Клас визначає клас мережі. Практично завжди це є ***IN***, що позначає ***INternet***.

Тип може бути одним з наступних:

- ***SOA*** — визначає ***DNS*** зону;
- ***NS***-сервер імен для зони;
- ***A*** — перетворення імені в ***IP***-адресу;
- ***PTR*** — перетворення ***IP***-адреси в ім'я;
- ***MX*** — поштова станція;
- ***CNAME*** — імена машини;
- ***HINFO*** — опис «заліза» комп'ютера;
- ***TXT*** — коментарі або якась інша інформація.

Є також деякі інші типи, але вони менш поширені.

У записах можна використовувати символи **#** та ***;*** для коментарів, **@** — для позначення поточного домену, ***()*** — дужки для написання даних на декількох рядках. Крім того, можна використати метасимвол ***** в імені. Порядок записів не має значення за одним виключенням: запис ***SOA*** повинен бути першим. Наступні записи вважаються стосовними до тієї ж зони, доки не зустрінеться новий запис ***SOA***. Як правило, після запису зони вказують записи ***DNS***-серверів, а інші записи абеткують, але це не обов'язково.

SOA — опис зони. Тепер спробуємо розглянути записи. Першою описуємо зону:

mycompany.ru. IN SOA ns.mycompany.ru. admin.mycompany.ru. (1001 ; serial
21600 ; Refresh - 6 годин
1800 ; Retry - 30 хв
1209600 ; Expire - 2 тижня
432000) ; Minimum - 5 днів

Спочатку йде ім'я домена: ***mycompany.ru.*** (зверніть увагу на крапку наприкінці імені). Замість імені можна було (і найчастіше так і роблять) поставити знак **@.**

ns.mycompany.ru. — основний сервер імен.

admin.mycompany.ru. — поштова адреса адміністратора у форматі ім'я(крапка)машина.

Потім у круглих дужках ідуть поля, необхідні для правильного «сприйняття» вашої зони іншими серверами. Перше число ***serial*** – є «версією» файлу зони. При внесенні змін це число треба збільшити — якщо вторинний сервер побачить, що його версія зони менше, ніж у первинного сервера, то він перечитає дані. Типовою помилкою є відновлення зони без відновлення цього числа. Дуже зручно в якості ***serial*** використати поточну дату, наприклад, ***2008040401*** — 4 квітня 2008 року, перше відновлення.

Refresh визначає як часто вторинні сервери повинні перевіряти значення ***serial***.

Retry визначає як часто вторинний сервер повинен намагатися прочитати дані, якщо первинний сервер не відповідає.

Expire визначає протягом якого часу вторинні сервери повинні обслуговувати домен, якщо первинний сервер не відповідає. Після закінчення цього часу вторинні сервери будуть вважати свої дані застарілими.

Minimum задає час життя записів за замовчуванням для даної зони.

NS описує сервери імен.

Тепер опишемо сервери імен, що обслуговують наш домен:

mycompany.ru. IN NS ns.mycompany.ru.

mycompany.ru. IN NS ns.provider.ru.

Оскільки ім'я зони збігається із зазначеним у полі ім'я запису ***SOA***, то його можна залишити порожнім.

Далі йдуть записи ***A***, що описують хости (комп'ютери) й дозволяють перетворити імена в ***IP***-адреси.

major IN A 192.168.0.1

colonel IN A 192.168.0.2

IN HINFO "2xPIV-1.7 Win2K"

general.mycompany.ru. IN A 192.168.0.3

Імена можуть бути відносні або «абсолютні», можна додати записи про конфігурацію машини (пропущене ім'я в записі ***HINFO*** говорить про те, що мається на увазі попереднє ім'я). Не забудьте додати записи

localhost. IN A 127.0.0.1

localhost IN CNAME localhost.

mycompany.ru. IN A 192.168.0.1

Перший запис повертає адресу ***127.0.0.1*** будь-якій машині, що запросила ім'я ***localhost***, другий — ***localhost.mycompany.ru***, а третій визначає, куди відправити запит клієнта, що хоче потрапити на ***mycompany.ru***

За допомогою ***CNAME*** можна задавати короткі імена серверів. Записи ***CNAME*** дозволяють дати машинам зручні або значущі імена. Наприклад:

ftp IN CNAME general означає, що ***ftp.mycompany.ru*** знаходиться за адресою ***192.168.0.3. CNAME*** зручно використовувати, якщо потрібно змінити ім'я машини, але хотіли б зберегти доступ для клієнтів, які пам'ятають старе ім'я. Зручний трюк з використанням ***CNAME*** полягає в призначенні коротких імен адресам, що часто використовуються. Наприклад, прописавши ***ls IN CNAME www.listsoft.ru.***, можна заходити на ***ListSoft*** просто набираючи ***ls*** як адресу.

MX описує пересилання пошти. Записи ***MX*** потрібні для того, щоб вказати, куди пересилати пошту. У цих записах додається пріоритет — чим менше параметр, тим вище пріоритет машини. Пріоритети потрібні для того, щоб можна було задати кілька записів і перенаправляти пошту на альтернативний сервер, якщо основний не працює. ***MX*** запис повинен бути зазначений для домену в цілому й, можливо, для кожної машини окремо. Дуже часто зустрічається неправильне використання метасимволу ***"*"***. Наприклад, запис ***"*.mycompany.ru."*** означає не "будь-яка машина домену ***mycompany.ru***",

а «будь-яка машина, що ще не була описана». Причому, навіть якщо використовувався не ***MX***, а, наприклад, ***A***-запис, то зірочка однаково не буде працювати для цієї машини. Більш докладно дізнатися про використання метасимволів можна в ***RFC 1034***, розділ 4.3.3. Загалом, метасимволи потрібні тільки для того, щоб приймати пошту для мережі, що перебуває за брандмауером і щоб пересилати пошту в мережі, не підключені до Інтернету (наприклад, що працюють через ***UUCP***). Через те, що записи ***DNS*** змінюються досить рідко, то має сенс прописати ***MX*** записи для всіх машин, описаних записами ***A***.

mycompany.ru. IN MX 10 relay
mycompany.ru. IN MX 20 mycompany.ru.
mycompany.ru. IN MX 30 mail.provider.ru.
general.mycompany.ru. IN A 192.168.0.3
IN MX 10 mycompany.ru.

На цьому створення файлу зони можна вважати закінченим, але залишається опис реверсної зони. Якщо попередній файл дозволяє визначити ***IP***-адресу за іменем, то тепер треба зробити так, щоб за ***IP***-адресою можна було «обчислити» ім'я. Відсутність реверсної зони є досить типовою помилкою й може призводити до найрізноманітніших помилок — починаючи від збоїв ***FTP***-серверів і закінчуючи класифікацією відправлених листів як спаму.

Для зворотнього перетворення використовуються записи ***PTR***. Але не поспішайте їх вписувати, адже вони пишуться в окремому спеціальному домені верхнього рівня з назвою ***IN-ADDR.ARPA***. Домен цей був створений для того, щоб і для прямого, і для зворотнього перетворень можна було використати однакові програмні модулі. Справа в тому, що «мнемонічні» імена пишуться зліва направо: ***www.listsoft.ru*** означає, що ***www*** перебуває в ***listsoft***, а ***listsoft*** — в ***ru***. ***IP***-адреси пишуться навпаки: ***195.242.9.4*** означає, що машина ***4*** перебуває в підмережі ***9***, що є частиною ***195.24.*** Для збереження «єдиного стилю» в адресі для зворотнього перетворення використовуються імена, що мають вигляд ***4.9.242.195.IN-ADDR.ARPA*** (зверніть увагу, що ***IP***-адреса записана у зворотньому порядку).

Отже, створюємо ще один файл зони (для зони, наприклад, ***0.168.192.IN-ADDR.ARPA***), копіюємо в нього запис ***SOA*** (а також й ***NS***), після чого починаємо писати:

1 IN PTR major.mycompany.ru.
2 IN PTR colonel.mycompany.ru.
...

Можна задавати не тільки відносні, але й абсолютні імена:

3.0.168.192.IN-ADDR.ARPA. IN PTR general.mycompany.ru.

Не забудьте ще задати зворотнє перетворення для ***127.0.0.1.***

Зверніть увагу на те, що право на ведення «прямого» домену не залежить від провайдера — його надає організація, що відає розподілом імен у потрібному вам домені. А ось пул ***IP***-адрес перебуває у віданні провайдера, і саме провайдер делегує (або не делегує) права на ведення реверсної зони. У

зв'язку з тим, що найчастіше клієнтам видається не ціла мережа класу ***«С»***, а її частина, то й реверсна зона перебуває на сервері провайдера. Так що доведеться налагодити з ним взаємодію в плані відновлення даних.

Для того, щоб подивитися, що записано в ***DNS***, використовується команда ***nslookup*** (вона є і в ***UNIX***, і в ***Windows***).

DNS має наступні характеристики:

- **Розподіленність зберігання інформації.** Кожен вузол мережі в обов'язковому порядку повинен зберігати тільки ті дані, які входять в його зону відповідальності й (можливо) адреси кореневих ***DNS***-серверів.
- **Кешірування інформації.** Вузол може зберігати деяку кількість даних не зі своєї зони відповідальності з метою зменшення навантаження на мережу.
- **Ієрархічна структура**, в якій всі вузли об'єднані в дерево, і кожен вузол може або самостійно визначати роботу нижчих в ієрархії вузлів, або делегувати (передавати) їх іншим вузлам.
- **Резервування.** За зберігання й обслуговування своїх вузлів (зон) відповідають (звичайно) декілька серверів, розділені як фізично, так і логічно, що забезпечує зберігання даних і продовження роботи навіть у випадку збою одного з вузлів.

Система ***DNS*** містить ієрархію серверів ***DNS***. Кожен домен або піддомен підтримується як мінімум одним авторизованим сервером ***DNS***, на якому розташована інформація про домен. Ієрархія серверів ***DNS*** збігається з ієрархією доменів. Ім'я хоста й ***IP***-адреса не тотожні — хост із однією ***IP***-адресою може мати безліч імен, що дозволяє підтримувати на одному комп'ютері безліч веб-сайтів (це називається віртуальний хостинг). Зворотнє теж справедливо — одному імені може бути зіставлено безліч хостів: це дозволяє створювати балансування навантаження. Крім того бувають реально працюючі ***IP***-адреси, яким не відповідає жодне ім'я.

Для підвищення стійкості системи використовується безліч серверів, що містять ідентичну інформацію. Існує 13 кореневих серверів, розташованих у всьому світі й прив'язаних до свого регіону, їхні адреси ніколи не змінюються, а інформація про них є в будь-якій операційній системі.

Протокол ***DNS*** використовує для роботи ***TCP*** або ***UDP***-порт 53 для відповідей на запити. Традиційно запити й відповіді відправляються у вигляді однієї ***UDP***-датаграми. ***TCP*** використовується у випадку, якщо відповідь більше 512 байт, або у випадку ***AXFR***-запиту.

DNS використовується в першу чергу для перетворення символьних імен в ***IP***-адреси, але він також може виконувати зворотний процес. Для цього використовуються вже наявні засоби ***DNS***. Справа в тому, що із записом ***DNS*** можуть бути зіставлені різні дані, у тому числі і яке-небудь символьне ім'я. Існує спеціальний домен ***in–addr.arpa***, записи в якому використовуються для перетворення ***IP***-адрес у символьні імена. Наприклад, для одержання ***DNS***-імені для адреси ***11.22.33.44*** можна запросити в ***DNS***-сервера запис ***44.33.22.11.in–addr.arpa***, і той поверне відповідне символьне ім'я. Зворотній

порядок запису частин ***IP***-адреси пояснюється тим, що в ***IP***-адресах старші біти розташовані на початку, а в символьних ***DNS***-іменах старші (що перебувають ближче до кореня) частини розташовані наприкінці.

DHCP (англ. ***Dynamic Host Configuration Protocol*** — протокол динамічної конфігурації вузла) — це мережевий протокол, що дозволяє комп'ютерам автоматично одержувати ***IP***-адресу та інші параметри, необхідні для роботи в мережі ***TCP/IP***. Для цього комп'ютер звертається до спеціального сервера, що називається сервером ***DHCP***. Мережевий адміністратор може задати діапазон адрес, що розподіляються серед комп'ютерів. Це дозволяє уникнути ручного настроювання комп'ютерів мережі й зменшує кількість помилок. Протокол ***DHCP*** використовується в більшості великих мереж ***TCP/IP***.

DHCP є розширенням протоколу ***BOOTP***, що використовувався раніше для забезпечення бездискових робочих станцій ***IP***-адресами при їхньому завантаженні. ***DHCP*** зберігає зворотну сумісність із ***BOOTP***.

Протокол ***DHCP*** надає три способи розподілу ***IP***-адрес:

- ***Ручний розподіл.*** При цьому способі мережевий адміністратор зіставляє апаратну адресу (звичайно ***MAC***-адресу) кожного клієнтського комп'ютера з певною ***IP***-адресою. Фактично, даний спосіб розподілу адрес відрізняється від ручного настроювання кожного комп'ютера лише тим, що відомості про адреси зберігаються централізовано (на сервері ***DHCP***), і тому їх простіше змінювати при необхідності.
- ***Автоматичний розподіл.*** При даному способі кожному комп'ютеру на постійне використання виділяється довільна вільна ***IP***-адреса з визначеного адміністратором діапазону.
- ***Динамічний розподіл.*** Цей спосіб аналогічний автоматичному розподілу, за винятком того, що адреса видається комп'ютеру не на постійне користування, а на певний строк. Це називається орендою адреси. Після закінчення строку оренди ***IP***-адреса знову вважається вільною, і клієнт зобов'язаний запросити нову (вона може виявитися тою ж самою).

Деякі реалізації служби ***DHCP*** здатні автоматично оновлювати записи ***DNS***, що відповідають клієнтським комп'ютерам, при виділенні їм нових адрес. Це виконується за допомогою протоколу відновлення ***DNS***, описаного в ***RFC 2136***.

Крім ***IP***-адреси, ***DHCP*** також може повідомляти клієнтові додаткові параметри, необхідні для нормальної роботи в мережі. Ці параметри називаються опціями ***DHCP***. Список стандартних опцій можна знайти в ***RFC 2132***. Ось деякі найбільш часто використовувані опції:

- ***IP***-адреса маршрутизатора за замовчуванням;
- маска підмережі;
- адреси серверів ***DNS***;
- ім'я домену ***DNS***.

Деякі постачальники програмного забезпечення можуть визначати власні, додаткові опції ***DHCP***.

Протокол ***DHCP*** є клієнт-серверним, тобто в його роботі беруть участь клієнт ***DHCP*** і сервер ***DHCP***. Передача даних виконується за допомогою протоколу ***UDP***, при цьому сервер приймає повідомлення від клієнтів на порт ***67*** і відправляє повідомлення клієнтам на порт ***68***. Всі повідомлення протоколу ***DHCP*** розбиваються на так звані поля, кожне з яких містить певну інформацію. Всі поля, крім останнього (поля опцій ***DHCP***), мають фіксовану довжину.

Розглянемо приклад процесу одержання ***IP***-адреси клієнтом від сервера ***DHCP***. Припустимо, клієнт ще не має власної ***IP***-адреси, але йому відома його попередня адреса — ***192.168.1.100***. Процес складається із чотирьох етапів.

1. Виявлення DHCP

На початку клієнт виконує широкомовний запит у всій фізичній мережі з метою виявити доступні ***DHCP***-сервери. Він відправляє повідомлення типу ***DHCPDISCOVER***, при цьому як ***IP***-адреса джерела вказується ***0.0.0.0*** (тому що комп'ютер ще не має власної ***IP***-адреси), а як адреса призначення — широкомовна адреса ***255.255.255.255***.

Клієнт заповнює кілька полів повідомлення початковими значеннями:

У полі ***xid*** міститься унікальний ідентифікатор транзакції, що дозволяє відрізняти даний процес одержання ***IP***-адреси від інших, що протікають у той же час.

У полі ***chaddr*** міститься апаратна адреса (***MAC***-адреса) клієнта.

У полі опцій вказується остання відома клієнтові ***IP***-адреса. У даному прикладі це ***192.168.1.100***. Однак це необов'язково і може бути проігноровано сервером.

Повідомлення ***DHCPDISCOVER*** може бути поширене за межі локальної фізичної мережі за допомогою спеціально налаштованих агентів ретрансляції ***DHCP***, що перенаправляють вхідні повідомлення від клієнтів ***DHCP*** серверам в інших підмережах.

2. Пропозиція DHCP

Одержавши повідомлення від клієнта, сервер визначає необхідну конфігурацію клієнта відповідно до заданих мережевим адміністратором настроювань. В даному випадку ***DHCP***-сервер згоден із запропонованою клієнтом адресою ***192.168.1.110***. Сервер відправляє йому відповідь (***DHCPOFFER***), в якому пропонує конфігурацію. Пропонована клієнтові ***IP***-адреса вказується в полі ***yiaddr***. Інші параметри (такі, як адреси маршрутизаторів й ***DNS***-серверів) вказуються у вигляді опцій у відповідному полі.

Це повідомлення ***DHCP***-сервер розсилає широкомовно. Клієнт може одержати кілька різних пропозицій ***DHCP*** від різних серверів; з них він повинен вибрати ту, що його «влаштовує».

3. Запит DHCP

Вибравши одну з конфігурацій, запропонованих ***DHCP***-серверами, клієнт відправляє запит ***DHCP*** (***DHCPREQUEST***). Він розсилається широкомовно; при цьому до опцій, зазначених клієнтом у повідомленні ***DHCPDISCOVER***,

додається спеціальна опція — ідентифікатор сервера, що вказує адресу ***DHCP***-сервера, обраного клієнтом (у цьому випадку — ***192.168.1.1***).

4. Підтвердження запиту DHCP

Нарешті, сервер підтверджує запит і направляє це підтвердження (***DHCPACK***) клієнтові. Після цього клієнт повинен настроїти свій мережевий інтерфейс, використовуючи надані опції.

DHCP-сервер надає адміністраторові ряд переваг. Головна — економія часу, що виникає за рахунок відмови від ручного конфігурування кожної машини. Нові комп'ютери найчастіше поставляються із встановленою ***ОС***. Якщо такий комп'ютер уже сконфігуровано як ***DHCP***-клієнт, можна підключити його до мережі, і йому відразу ж буде автоматично призначена ***IP***-адреса. Якщо ні, то програма інсталяції при одержанні позитивної відповіді на відповідне питання сама сконфігурує систему, як ***DHCP***-клієнт. Якщо призначити ***IP***-адреси вручну, необхідно зберігати список уже виданих адрес. Адміністратори нерідко носять такі списки із собою, тому що вони можуть знадобитися їм при конфігуруванні нових комп'ютерів. Якщо на підприємстві кілька адміністраторів, їм доводиться ще й координувати один з одним призначення адрес. ***DHCP*** знає, яким комп'ютерам які адреси призначені. Адміністраторам більше не знадобиться побоюватися помилок при введенні адрес і випадкового призначення тієї самої адреси декільком комп'ютерам.

DHCP спрощує й інші адміністративні завдання. Зокрема, можна з легкістю зможете переміщувати комп'ютер з однієї підмережі в іншу. При необхідності передати кому-небудь комп'ютер з нього можна буде попередньо скопіювати конфігураційні файли на іншій. Якщо не користуватися ***DHCP***, то обидва комп'ютери мали б у результаті ті самі ***IP***-адреси. ***DHCP*** усуває цю проблему й скорочує кількість звернень до служби підтримки.

Є в ***DHCP*** переваги й для користувачів. Користувачі ноутбуків, наприклад, не зможуть підключитися до мережі, якщо адреси видаються вручну. Однак клієнти, що підтримують ***DHCP***, при підключенні відразу ж одержують нові дійсні ***IP***-адреси.

Крім того, ***DHCP*** дозволяє здійснювати спільне використання ***IP***-адрес. Припустимо, у вас є 50 вільних адрес і відділ збуту зі штатом в 100 чоловік. Співробітники відділу проводять в офісі всього 1-2 дні на тиждень; таким чином, одночасно до мережі завжди підключені тільки 30-40 комп'ютерів. Щоразу при підключенні до мережі співробітник одержує ***IP***-адресу. Після відключення система звільнює адресу, щоб призначити її наступному користувачеві.

Якщо декілька мобільних користувачів ділять між собою кілька ***IP***-адрес, деяку їхню кількість можна зарезервувати для тих, кому вони найбільше потрібні. Відкрийте діалог ***DHCP Manager***, виберіть ***Scope, Add Reservations***. Таким чином можна зарезервувати адресу для комп'ютера з певним мережним адаптером. Це може створити певні труднощі, якщо користувачі поміняються адаптерами. Резервування має свої відмінності від присвоєння фіксованої ***IP***-адреси. Резервування так само надає користувачеві можливість підключатися

до мережі в різних відділах, але адреса залежно від місця розташування може змінюватися.

Хід роботи

1. Порівняйте процедури дозволу імен, способи завдання імен комп'ютерів, обмеження, що накладаються на імена в ***DNS*** й ***NetBIOS***.

2. Очистіть кеши дозволу імен, як протоколу ***DNS***, так й ***NetBIOS***, за допомогою команд ***ipconfig /flushdns*** й ***nbtstat –R***, відповідно(рисунок 4.1).Запустіть запис трафіку в ***Мережевому моніторі***(рисунок 4.2). У командному рядку виконайте команду ***ping <сусідній комп'ютер>***. Одержавши 4 відгуки, закінчіть запис трафіку. Збережіть результати у файлі ***NameResolution1***.

```
C:\Users\Administrator>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\Administrator>nbtstat -r

    NetBIOS Names Resolution and Registration Statistics
    ----------------------------------------------------

    Resolved By Broadcast      = 0
    Resolved By Name Server    = 0

    Registered By Broadcast    = 6
    Registered By Name Server  = 0

C:\Users\Administrator>ping 10.100.0.1

Pinging 10.100.0.1 with 32 bytes of data:
Reply from 10.100.0.1: bytes=32 time=1ms TTL=62
Reply from 10.100.0.1: bytes=32 time=1ms TTL=62
Reply from 10.100.0.1: bytes=32 time=1ms TTL=62
Reply from 10.100.0.1: bytes=32 time=1ms TTL=62

Ping statistics for 10.100.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

Рисунок 4.1 – Очистка кешу дозволу імен

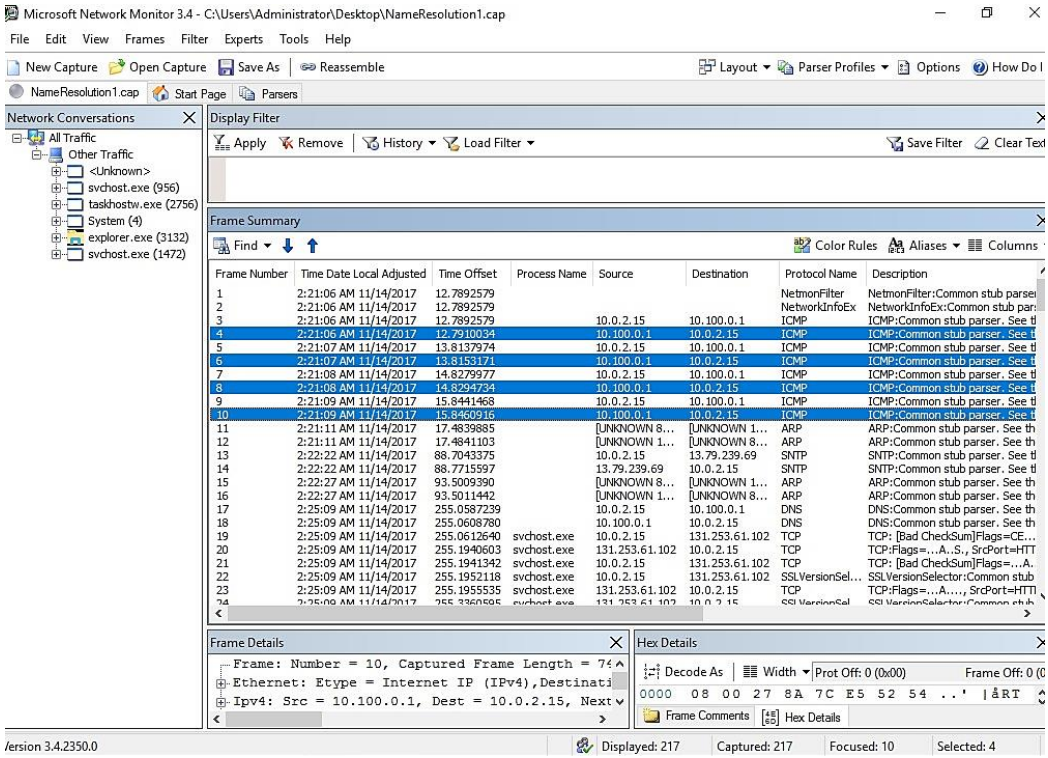

Рисунок 4.2 – Запуск запису трафіку в Мережевому моніторі

3. Вивчіть архітектуру ***DNS***. Вивчіть механізм роботи кешу, як на ***DNS***-серверах, так і на ***DNS***-клієнтах.

4. Додайте серверну роль ***DNS-сервер***. На сторінках майстра настроювання ***DNS***-сервера залиште всі значення, задані за замовчуванням. Іншим способом додавання ролі є встановлення компонента ***DNS***-сервер за допомогою утиліти ***Додати ролі та компоненти*** (рисунок 4.3). Скористайтеся саме цим способом, тому що згодом потрібно налаштувати сервер вручну.

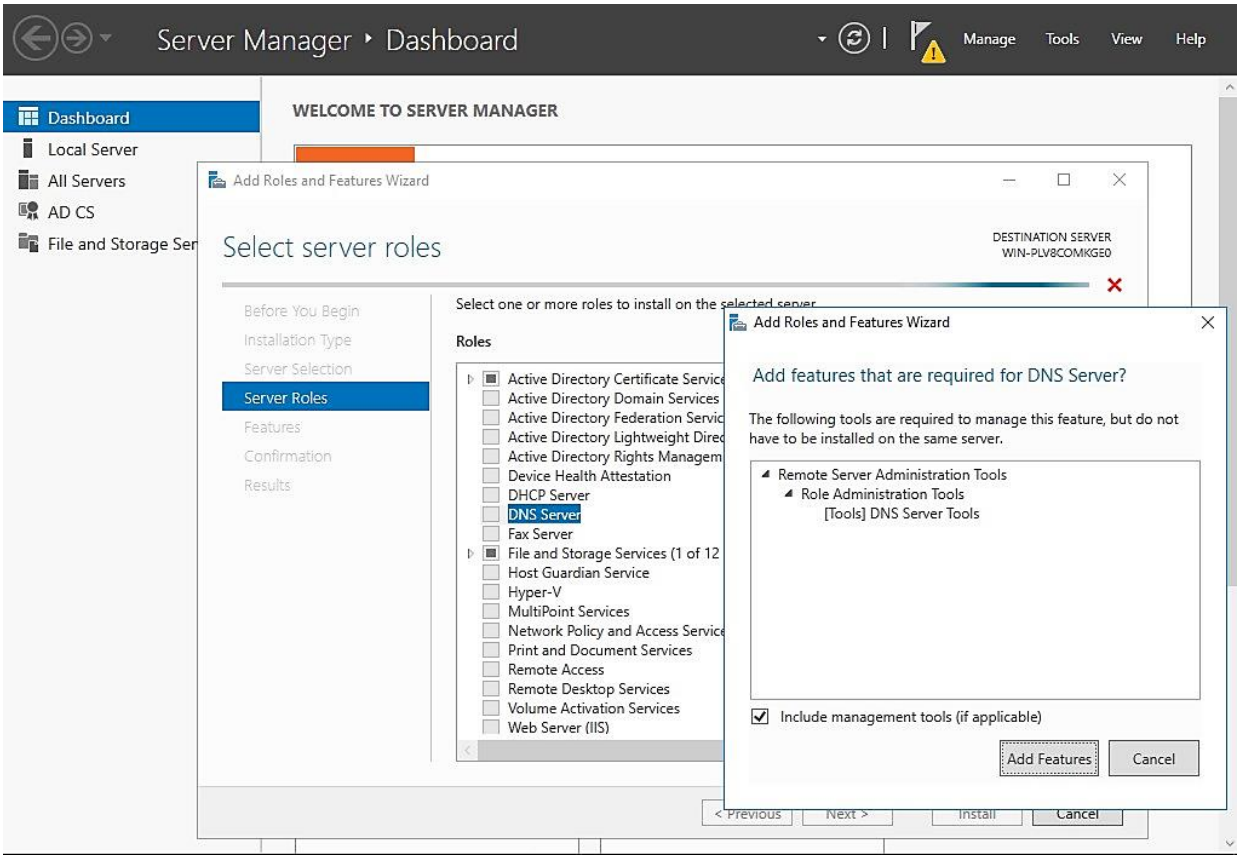

Рисунок 4.3 – Додавання ролі DNS-сервер

5. Переконайтеся, що налаштували комп'ютер на звертання до вищого в ієрархії ***DNS***-сервера (наприклад, сервера Інтернет-провайдера). У дереві консолі ***DNS*** у контекстному меню комп'ютера виберіть пункт ***Настроїти DNS-сервер***. У майстрі оберіть варіант ***Створити зони прямого й зворотнього перегляду***(рисунок 4.4). Укажіть тип зони: ***Основна***. Задайте осмислене ім'я зони (таблиця 4.1. На даному етапі забороніть динамічні відновлення. Для зони зворотнього перегляду (рисунок 4.5) визначте ***Код мережі*** згідно таблиці 4.1. Не вказуйте сервери пересилання.

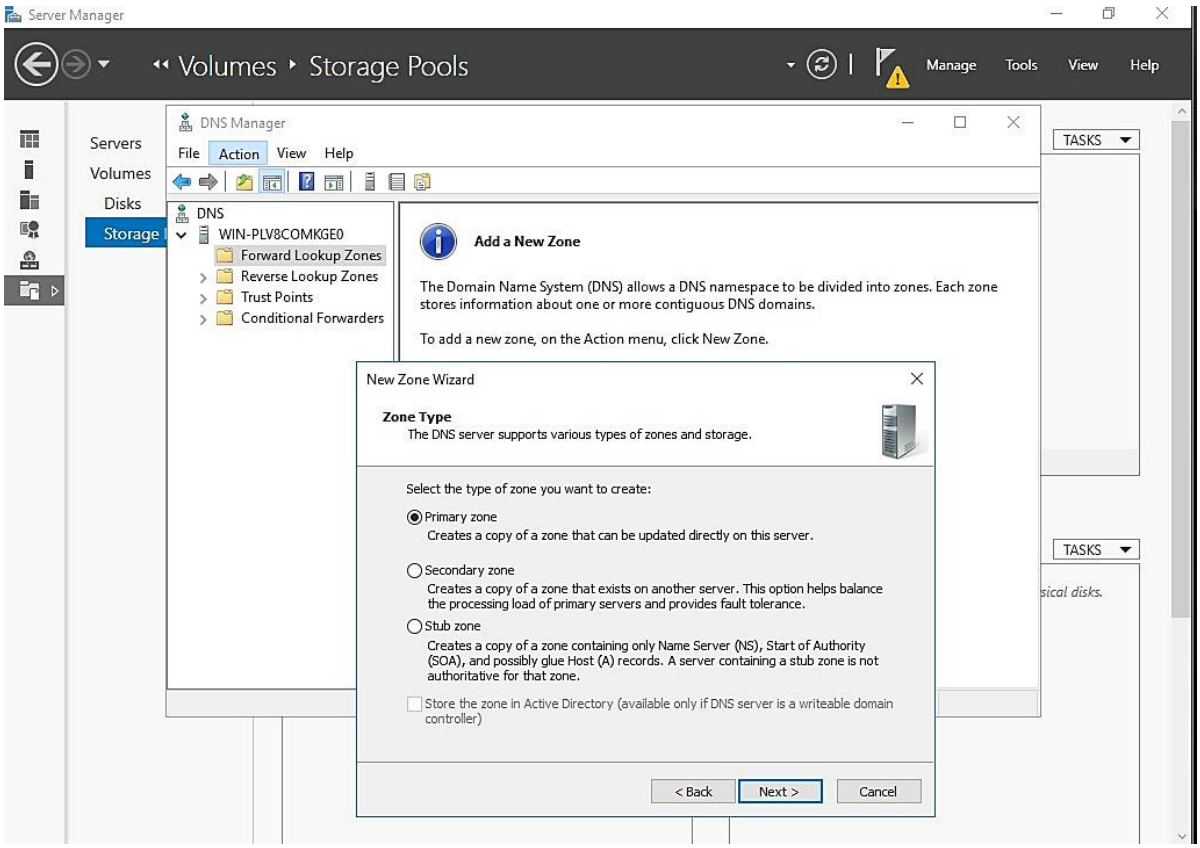

Рисунок 4.4 – Створення зони прямого перегляду

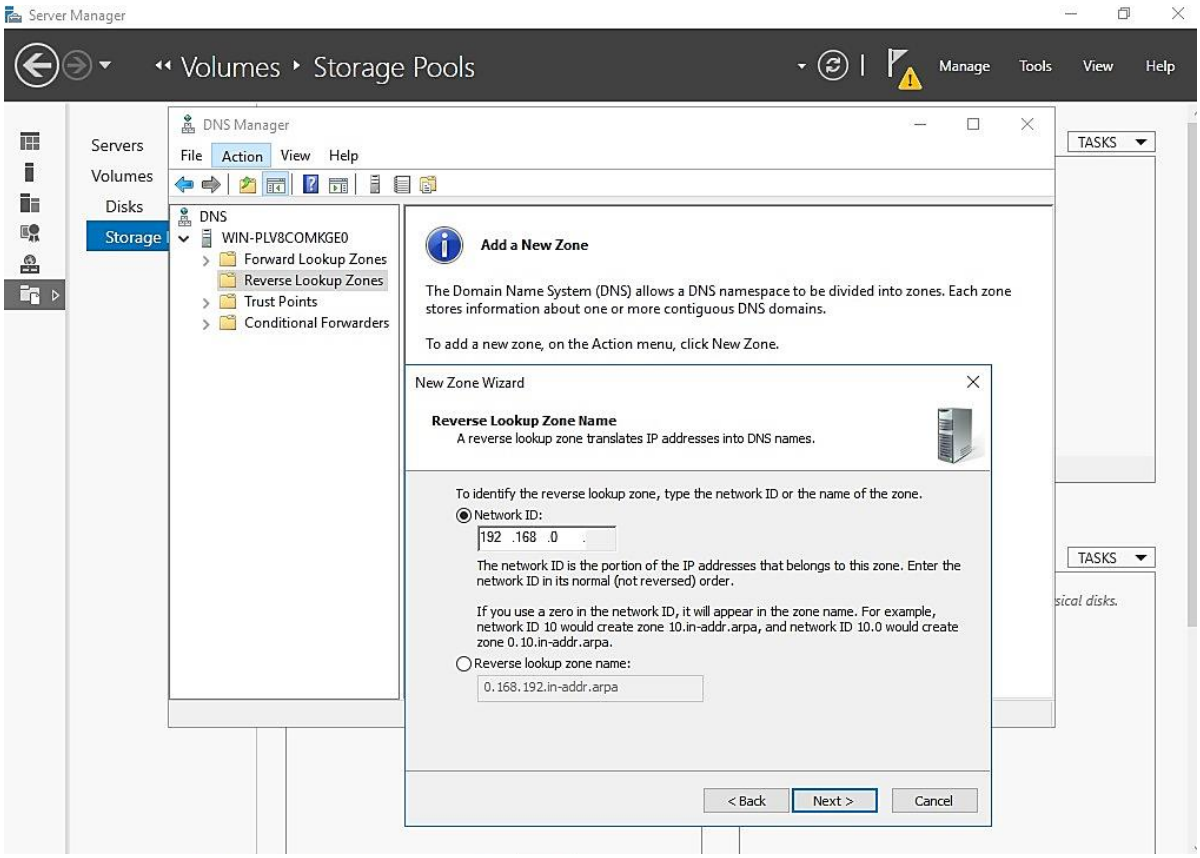

Рисунок 4.5 – Створення зони зворотнього перегляду

6. Зайдіть у властивості комп'ютера в консолі ***DNS***. На вкладці ***Спостереження*** вивчіть можливості й способи застосування двох тестів. Виконайте обидва тести й проаналізуйте результати (рисунок 4.6).

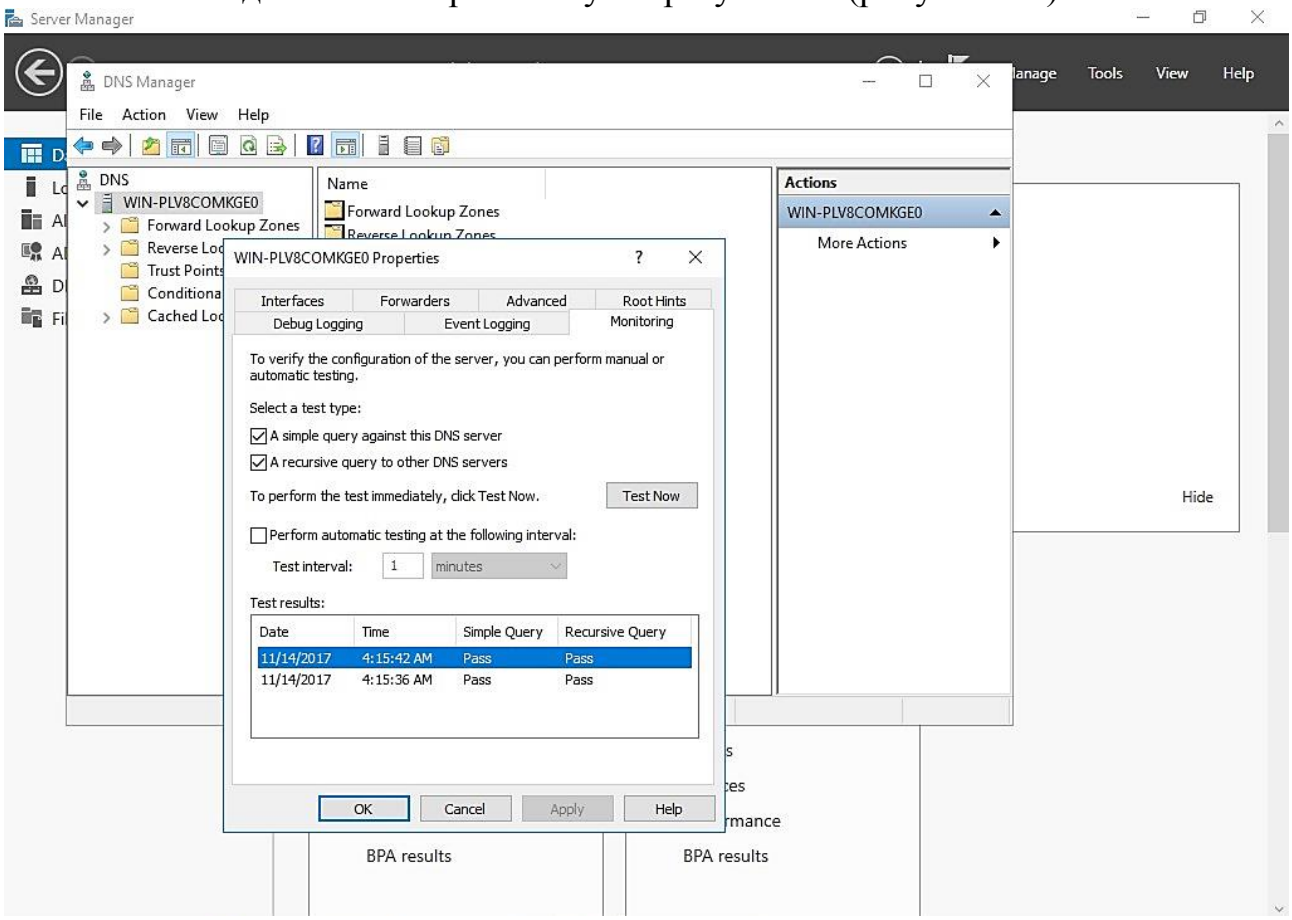

Рисунок 4.6 – Виконання тестів

7. Задайте ***DNS***-суфікс на двох комп'ютерах таким, як була названа створена зону (наприклад, ***net1.local***). Застосування змін потребуватиме перезавантаження. Перевірте за допомогою команди ***ping <сусідній комп'ютер>***, як тепер дозволяється ім'я. Проаналізуйте як змінився суфікс (рисунок 4.7).

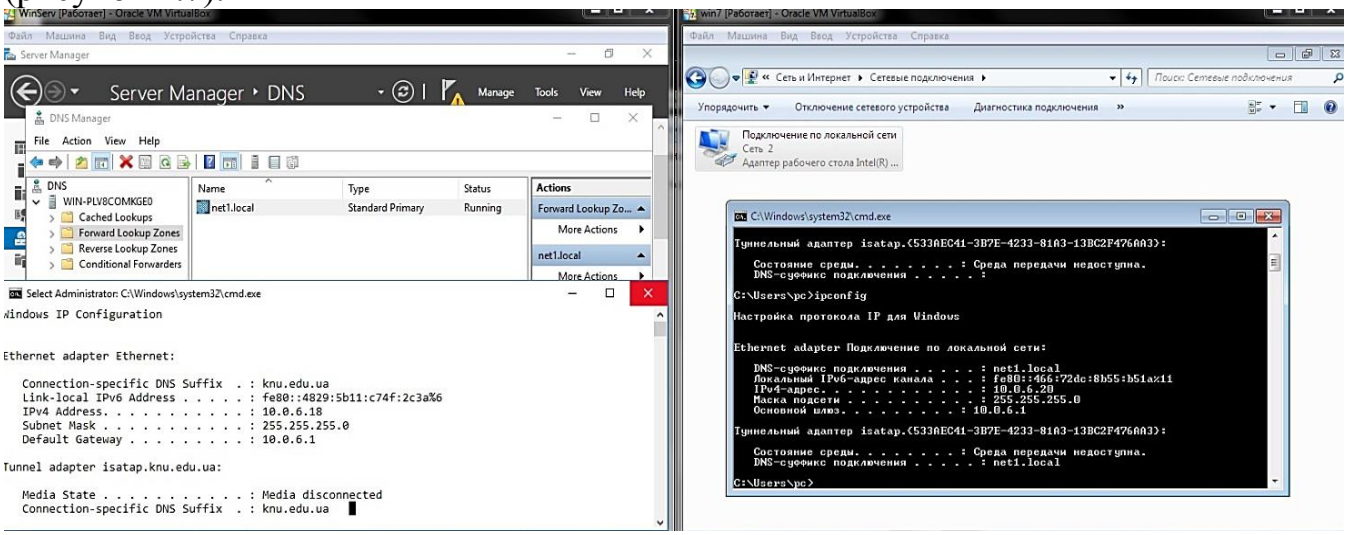

Рисунок 4.7 – Перевірка зміни DNS-суфіксу

8. Для перевірки рекурсії буде потрібний доступ до вищого в ієрархії ***DNS***-сервера (Інтернет).

На даному етапі такий доступ можна організувати за допомогою служби ***ICS***, що забезпечить перетворення локальних адрес у зовнішні. Для включення ***ICS*** поставте прапорець ***«Дозволити іншим користувачам мережі використати підключення до Інтернету даного комп'ютера»*** на вкладці ***«Додатково»*** властивостей підключення. Пам’ятайте, що ***ICS*** сильно обмежує структуру локальної мережі.

9. Запустіть запис ***Мережевого монітору***.

10. Виконайте команди ***ipconfig /all*** й ***ipconfig /flushdns.*** Тепер у браузері спробуйте відкрити будь-яку існуючу адресу. Якщо доступ до цієї адреси можливий, з'єднання пройде успішно.

11. Закінчіть запис трафіку. Відшукайте пакети з ***DNS***-запитами. Визначте, які прапори встановлені, які скинуті. Зайдіть у дерево ***DNS***, перемикніться в режим розширеного перегляду й відкрийте розділ ***Кешовані перегляди***. Проаналізуйте й поясніть зміни, що відбулися в кеші.

Таблиця 4.1 – Варіанти завдання

№ варіанту	Ім'я зони	Код мережі
1	net1.local	192.168.0
2	net2.local	192.168.1
3	net3.local	192.168.2
4	net4.local	192.168.3
5	net5.local	192.168.4
6	net6.local	192.168.5
7	net7.local	192.168.6
8	net8.local	192.168.7
9	net9.local	192.168.8
10	net10.local	192.168.9

12. ***ICS*** має власну ***DHCP***-подібну функцію призначення адрес. Вона несумісна зі службою ***DHCP*** і повинна бути відключена перед розгортанням ***DHCP***-сервера. Вимкніть підключення віддаленого доступу на комп'ютері.

13. На клієнтському комп'ютері встановіть статичну адресу та й адресу ***DNS***-сервера згідно таблиці 4.2. Перезавантажте комп'ютер.

14. На сервері задайте статичну адресу згідно таблиці 4.2. Зверніть увагу, раніше комп'ютер також мав 192 адресу.

15. Додайте роль ***«DHCP-сервер»*** за допомогою майстра ***«Керування даним сервером»***. Задайте новій області осмислене ім'я й діапазон адрес згідно таблиці 4.2(рисунок 4.8). Додайте виключення згідно таблиці 4.2(рисунок 4.9). Термін дії оренди залиште без змін (8 днів). Задайте адреси шлюзу, ***DNS***-сервера й ***WINS***-сервера у відповідності з таблицею 4.2. Задайте параметру ***«Батьківський домен»*** ім'я, що був призначений домену при створенні (наприклад, ***net1.local***) (рисунок 4.10). Зверніть увагу, що всі ці параметри можна задати як для області, як для суперобласті, так і для всього серверу.

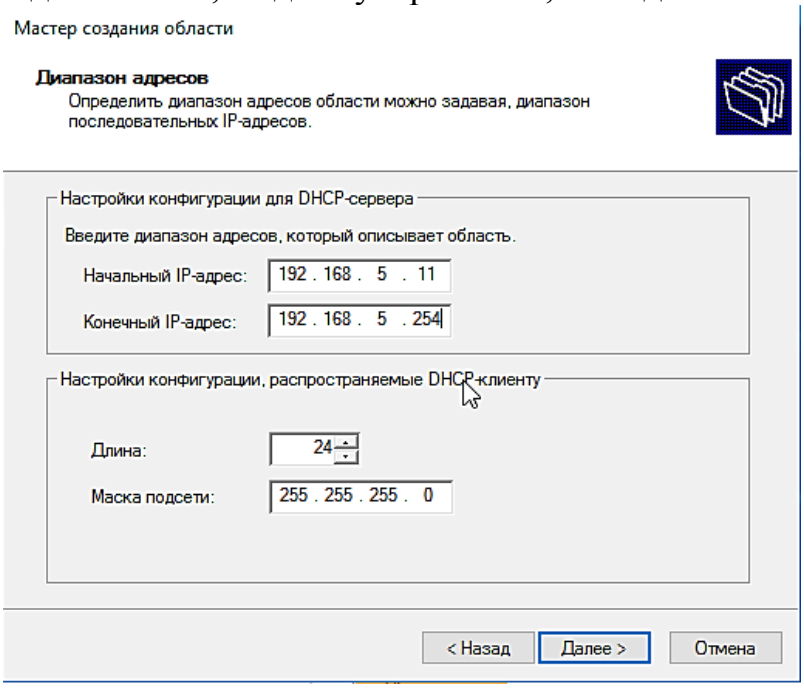

Рисунок 4.8 – Задання діапазону адрес

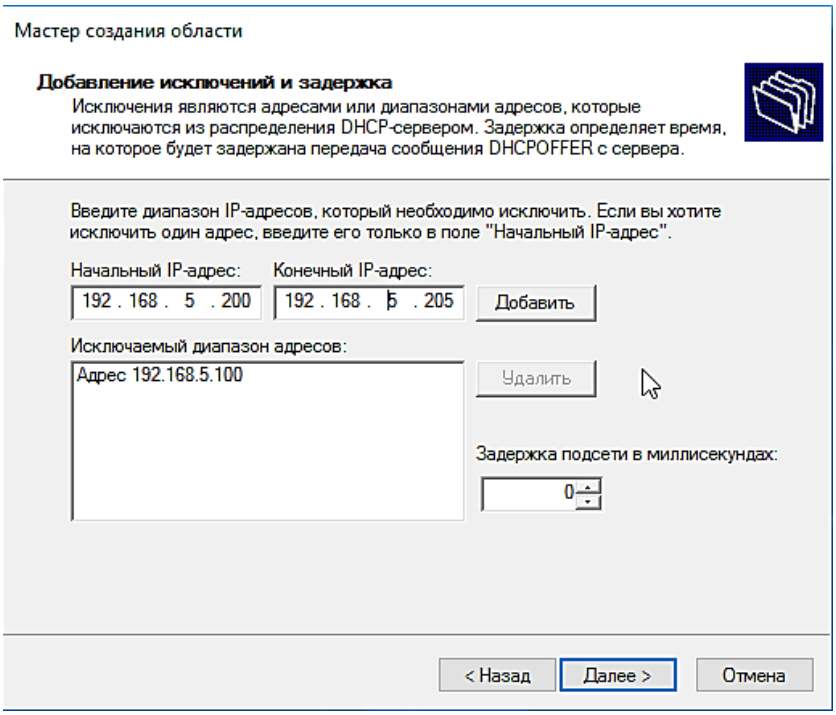

Рисунок 4.9 – Додання виключення адрес

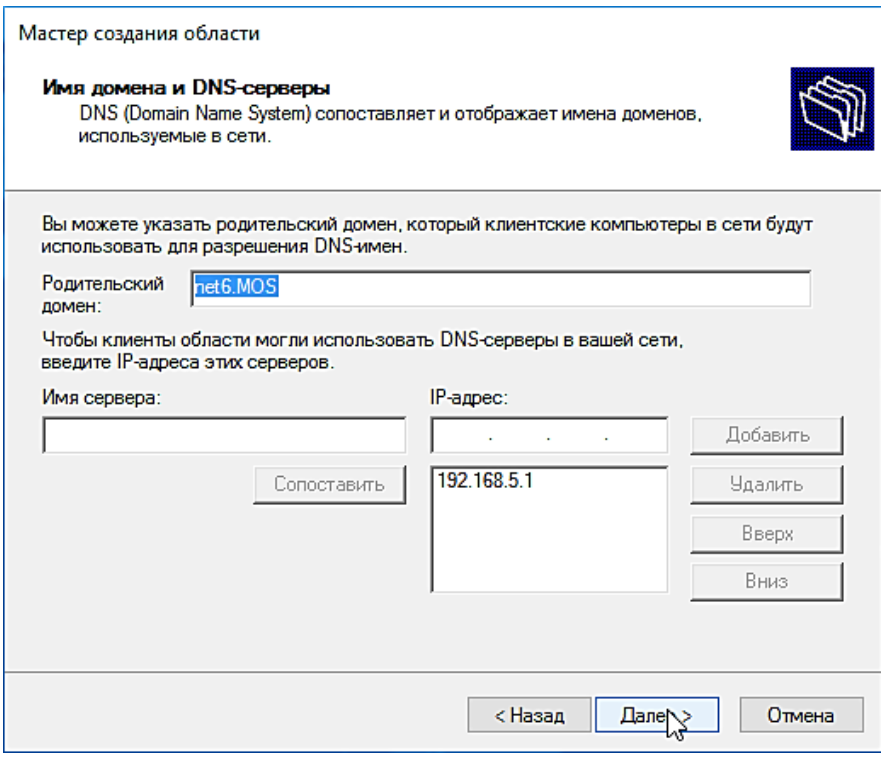

Рисунок 4.10 – Задання параметру «Батьківський домен»

16. Активізуйте створену область. Для цього, можливо, буде потрібно авторизувати ***DHCP***-сервер. Працюючий сервер відзначається зеленою стрілкою нагору.

17. Знищіть будь-які ресурсні записи типів ***A*** й ***PTR*** для сусіднього комп'ютера з ***DNS***, а також з кешу. ***DHCP***-сервер буде самостійно заносити нові записи при виділенні адрес. У властивостях ***TCP/IP*** відзначте варіанти ***«Одержати IP-адресу автоматично»*** й ***«Одержати адресу DNS-сервера автоматично».*** Виконайте команду ***ipconfig /registerdns***.

18. Виконайте команду ***ipconfig.*** Ознайомтеся з новою конфігурацією хоста(рисунок 4.11).

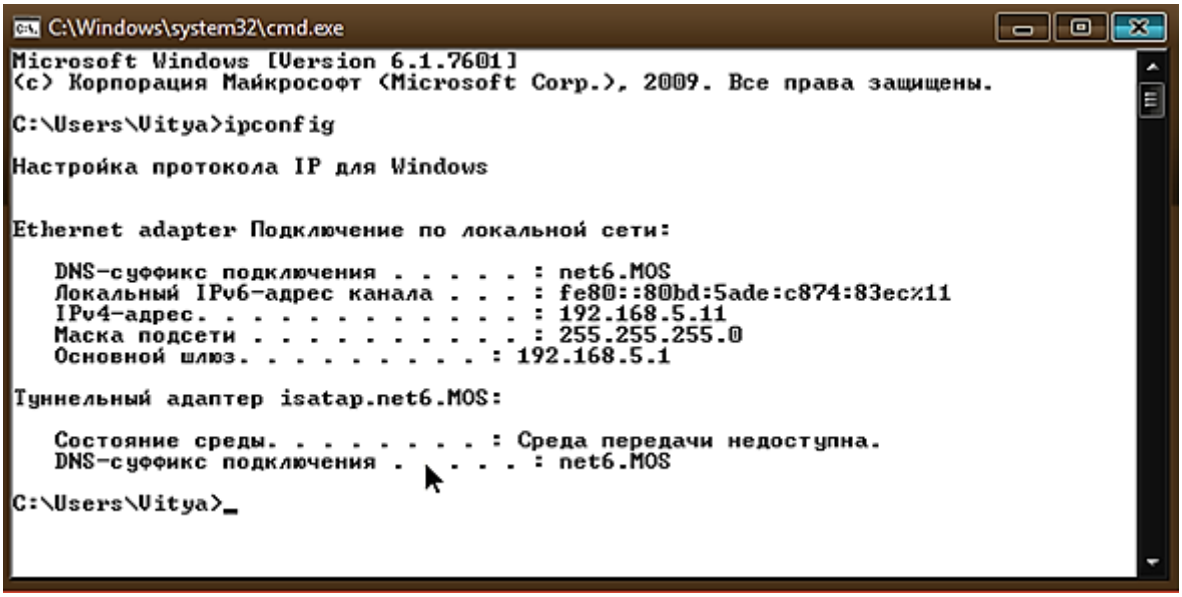

Рисунок 4.11 – Нова конфігурація хоста

19. У контекстному меню вузла ***DHCP***-сервера консолі ***DHCP*** виберіть ***«Архівувати»*** й збережіть архів в обраній папці. Ознайомтеся з можливостями й призначенням утиліти ***jetpack***. Застосуйте її для стиснення бази даних ***DHCP***-сервера. При цьому служба ***DHCP*** повинна бути відключена. Приклад послідовності команд:

cd %windir%\system32\dhcp
net stop dhcpserver
jatpack dhcp.mdb tmp.mdb
net start dhcpserver

20. Розберіться в способі застосування класів постачальників і класів користувачів. Ознайомтеся із уже наявними класами, зайшовши у відповідні вікна через контекстне меню вузла сервера. Додайте новий клас користувачів, наприклад, ***«Мобільні».*** Задайте для цього класу сильно скорочений строк оренди адреси (наприклад, 4 години). Така політика широко використовується на підприємствах. Не рідко виникає необхідність призначити деяким користувачам особливий шлюз за замовчуванням для доступу в Інтернет. Використайте команду ***ipconfig /setclassid*** для вказівки приналежності до класу.

21. У консолі ***DHCP*** у контекстному меню сервера оберіть ***«Створення суперобласті».*** В майстрі задайте їй осмислене ім'я й додайте наявну область. Додайте до суперобласті іншу область (наприклад, для першої бригади — ***192.168.0.2–8/24***). Тепер сервер може видавати адреси з обох областей. У конфігурації не потрібна ні друга область, ні суперобласть. Видаліть їх. Увага! Спочатку завжди знищується суперобласть, а потім області, що входять в неї. Суперобласть ***НЕ Є*** батьком областей у звичному розумінні.

22. Запустіть запис трафіку. Виконайте команду ***ipconfig /release*** на сусідньому комп'ютері. Проаналізуйте результати. Виконайте команду ***ipconfig /renew***. Зупиніть запис і відобразьте дані. Задайте фільтр відображення так, щоб ***DHCP*** був єдиним включеним протоколом. Збережіть запис під іменем ***DHCPLeaseInit***, встановивши прапорець ***«Фільтр».*** Проаналізуйте отримані пакети. Повторіть завдання спочатку, виконавши на сусідньому комп'ютері тільки команду ***ipconfig /renew.*** Збережіть запис у файлі ***DHCPLeaseRenew.*** Проаналізуйте отримані пакети.

Таблиця 4.2 – Варіанти завдання

№ варіанту	Ім'я домену	IP-адреса сервера (шлюзу, DNS-та WINS-сервера)	Статична IP-адреса клієнта	Діапазон IP-адрес	Виключення
1	net1	192.168.0.1	192.168.0.2	192.168.0.11–254/24	192.168.0.100 та 192.168.0.200-205
2	net2	192.168.1.1	192.168.1.2	192.168.1.11–254/24	192.168.1.100 та 192.168.1.200-205
3	net3	192.168.2.1	192.168.2.2	192.168.2.11–254/24	192.168.2.100 та 192.168.2.200-205
4	net4	192.168.3.1	192.168.3.2	192.168.3.11–254/24	192.168.3.100 та 192.168.3.200-205
5	net5	192.168.4.1	192.168.4.2	192.168.4.11–254/24	192.168.4.100 та 192.168.4.200-205
6	net6	192.168.5.1	192.168.5.2	192.168.5.11–254/24	192.168.5.100 та 192.168.5.200-205
7	net7	192.168.6.1	192.168.6.2	192.168.6.11–254/24	192.168.6.100 та 192.168.6.200-205
8	net8	192.168.7.1	192.168.7.2	192.168.7.11–254/24	192.168.7.100 та 192.168.7.200-205
9	net9	192.168.8.1	192.168.8.2	192.168.8.11–254/24	192.168.8.100 та 192.168.8.200-205
10	net10	192.168.9.1	192.168.9.2	192.168.9.11–254/24	192.168.9.100 та 192.168.9.200-205

Звіт повинен включати:

1. Тему, мету і порядок роботи.
2. Опис виконання усіх дій.
3. Висновки.

Контрольні питання:

1. Коли обов'язкове використання ***DNS***? Коли ***NetBIOS***? Які наслідки спричинить відключення ***NetBIOS*** на комп'ютерах?

2. Як ***DFS*** дозволяє вирішити завдання розподілу файлових ресурсів між рядовими комп'ютерами без використання ***NetBIOS***?
3. Що собою прежставляють простори імен? Як формуються доменні імена? Як організовано систему імен в Інтернеті?
4. Які існують типи ***DNS***-серверів? Які функції вони виконують?
5. Поясніть будову зони ***DNS***, типи записів ресурсів. Для чого служать такі записи ресурсів, як ***A, CNAME, NS, MX, PTR, SRV***?
6. Коли й ким виконуються рекурсивні ***DNS***-запити?
7. Як використовуються кореневі посилання?
8. Визначте різницю між зонами прямого й зворотнього перегляду. У чому полягають їхні загальні риси?
9. Розкажіть про можливі типи серверів: ***Основні***, ***Додаткові***, ***Зони-заглушки***, ***Кешуючі***.
10. У чому особливість інтеграції основної зони з ***Active Directory***?
11. Де можна задати основний суфікс комп'ютера?
12. Де задаються суфікси окремих підключень?
13. У якому порядку відбувається підстановка суфіксів при дозволі імені?
14. Що таке область? Що таке суперобласть?
15. Що таке активація й авторизація областей? У якому випадку авторизація необхідна?
16. Що таке резервування? Як буде працювати виділення адреси, якщо резервована адреса підпадає в діапазон виключень?
17. У чому відмінність архівування стиску бази даних ***DHCP***? Як можна відновити базу на сервері? Як можна перенести функціонуючий ***DHCP***-сервер на іншу фізичну машину?
18. Скільки класів користувачів можна призначити клієнтському комп'ютеру? Як ***DHCP***-сервер довідається, до якого класу користувачів належить клієнтський комп'ютер?
19. Як називаються п'ять ***DHCP***-повідомлень? У якому порядку вони генеруються?
20. Зі скількох пакетів складається процес відновлення оренди? Як вони називаються й в якому порядку генеруються? Яке конкретне поле якого ***DHCP***-повідомлення оновлює ***DHCP***-параметри конфігурації клієнта?

ЛАБОРАТОРНА РОБОТА №5

Тема: «Встановлення та настроювання служби каталогів Active Directory».

Мета: розглянути практичні аспекти встановлення, настроювання та адміністрування служби каталогу Microsoft Windows 2016 Active Directory, навчитись застосувати на практиці технології групових політик Group Policy для централізованого керування користувачами та ресурсами мережі.

Теоретичні відомості

Active Directory (AD) — це ієрархічно організоване сховище, що надає зручний доступ до відомостей про різні об'єкти мережі, допомагаючи користувачам і додаткам знайти ці об'єкти. До того ж він перевіряє, чи є в користувача, що запросив інформацію, право на її одержання. Список прав користувачів також знаходиться в базі даних ***Active Directory***.

Комп'ютер, на якому працює сервер каталогу, називається ***контролером домену***; іншими словами, контролер домену — це комп'ютер, на якому розміщена вся база даних ***Active Directory***. Всі запити до активного каталогу й взагалі всі запити, що стосуються доступу до інформації, що зберігається в домені, обробляє саме цей комп'ютер. Роль керування доменом — настільки важлива в мережі функція, що від неї прямо залежить робота мережі. Тому й доступ до ***контролерів домена*** (***DC, Domain Controller***) дозволяється з більшою обережністю, ніж до інших, а самі ці комп'ютери більш захищені (як з погляду мережного доступу, так і чисто фізично) та оснащуються найнадійнішим устаткуванням. У великих мережах вони ніколи не виконують додаткових серверних функцій (не бувають серверами друку, додатків, файловими серверами й т.п.). Реалізація доменної моделі мережі починається з встановлення контролера домена. Оскільки ніяке устаткування не має стовідсоткової гарантії, може трапитися, що через певний час контролер домену вийде з ладу. Очевидно, що база даних ***Active Directory*** перестане бути доступною, а це значить, що користувачі не зможуть зареєструватися на жодному з комп'ютерів домену. До таких неприємностей потрібно готуватися ще на етапі планування мережі, і рішенням буде організація декількох контролерів домену.

Обліковий запис користувача повинний забезпечувати його роботу в усьому просторі домену. Якщо в домені кілька контролерів, то його облікові записи зберігаються на декількох комп'ютерах. При цьому протиріч не виникає, оскільки при встановленні другого контролера домену не створюється нової бази даних ***Active Directory***, замість цього на нього копіюється (цей процес називається ***реплакацією***) існуюча база даних. Таким чином, кожний контролер домену зберігає однакові дані, включаючи облікові записи користувачів. Тепер, якщо один з контролерів домену вийде з ладу, клієнти автоматично перемкнуться на інший, і це анітрохи не перешкодить їхній роботі.

До деяких мереж висуваються вимоги, які не може задовільнити один домен. Справа навіть не в тому, що максимальна кількість об'єктів в активному каталозі обмежена: в обмеження в кілька мільйонів об'єктів не вписатися важко.

Адже це не домен операційної системи ***Windows NT 4.0***, в якому могло перебувати не більше сорока тисяч об'єктів. Домен ***Windows Server 2016*** можна вважати практично безрозмірним. Але обставини, при яких доречною або неминучою буде організація ще одного домена, існують. От кілька прикладів:

- Адміністративне рішення. Технічних причин у цьому випадку немає, але вимогу керівництва підприємства виконувати потрібно.
- Різні вимоги до безпеки в різних підрозділах. Наприклад, якщо керівництво вимагає, щоб у користувачів з відділу розробки пароль був не коротше 10 символів, а у всіх інших — не коротше 8 символів, то ці вимоги в межах одного домена виконати неможливо. Доведеться виділяти розроблювачів в інший домен.
- Різні підрозділи повинни бути представлені в Інтернеті під різними іменами. Один домен не може мати декількох імен.
- Перевантаження ліній зв'язку. Коли в домені створюється новий об'єкт (наприклад, обліковий запис користувача), то він реплицюється на всі контролери домена. Якщо на підприємстві два підрозділи, зв'язані між собою повільною й ненадійною лінією, то не варто завантажувати цю лінію ще й копіюванням вмісту активного каталогу: тут доречно виділити ці підрозділи в окремі домени.

На практиці можна зустріти середовище, у розпорядженні якого є декілька доменів. Мова йде про закордонні відділення компаній або про дуже великі підприємства. Однак якщо ваше підприємство не відповідає якій-небудь із вищеописаних ситуацій, то вам вистачатиме й одного домену.

Якщо у вашій організації декілька доменів, у вас є дві можливості їхньої логічної організації. Перша з них називається ***деревом доменів***. Вона характеризується тим, що домени, що входять у дерево, утворюють єдиний простір імен. Це значить, що імена об'єктів повинні бути унікальними в межах усього дерева. Досягається ця унікальність тим, що повне ім'я підлеглого домену ***(europe.microsoft.com)*** складається з його власного імені ***(europe)*** і імені вищого в ієрархії домена ***(microsoft.com).*** Ім'я домена вищого рівня ***(кореневого домену)*** входить в імена всіх піддоменів.

На кількість доменів, що утворять дерево, обмежень немає.

Домени можуть бути пов'язані один з одним довірчими відносинами. Довірчі відносини означають наступне: користувач, що має обліковий запис у домені-довіренному, автоматично одержує доступ до поділюваних ресурсів домену-доверітеля. Відношення довіри транзитивно: якщо домен ***A*** довіряє домену ***B***, а домен ***B*** довіряє домену ***C***, то домен ***A*** довіряє домену ***C***.

При створенні декількох доменів в одному дереві ***Active Directory*** автоматично встановлюються міждоменні двонаправлені довірчі відносини. Новий домен, що орагнізується в рамках дерева, автоматично вступає в довірчі відносини зі старими, причому ці відносини двонаправлені: якщо домен ***A*** довіряє домену ***B***, то домен ***B*** довіряє домену ***A***. Таким чином, користувач може, зареєструвавшись тільки в одному домені, одержати доступ до всіх ресурсів всіх доменів дерева.

У порівнянні з ***Windows NT*** правила іменування доменів ***Active Directory*** змінилися: тепер імена доменів ***Active Directory*** виглядають так само, як імена доменів Інтернету. Якщо домен ***Windows NT*** міг називатися ***company***, то ім'я домена ***Active Directory*** повинне мати хоча б один суфікс: ***company.corn*** або ***company.local.*** Саме ім'я ***company*** — це ім'я ***NetBIOS***, у той час, як ***company.com*** — це ім'я ***DNS***. Починаючи з ***Windows 2000***, імена ***DNS*** стали основним засобом іменування вузлів мережі; більш ранні версії ***ОС Windows*** використовують переважно ***NetBIOS***-імена. З метою зворотної сумісності потрібно було узаконити обидва варіанти імені домена, і в ***Active Directory*** так і зроблено: клієнтським комп'ютерам під керуванням ***Windows NT 4.0 Workstation*** домен буде відомий як ***company***, а клієнтам під керуванням ***Windows XP Professional*** — як ***company.com.***

Якщо вирішили встановлювати домен ***Active Directory*** у системі ***Windows 2000 Server***, потрібно насамперед ретельно вибрати для нього ім'я, адже потім його неможливо буде поміняти. Ім'я кореневого домену є «електронною візитною карткою» підприємства. Воно входить складовою частиною в імена інших доменів того ж дерева. При його виборі необхідно враховувати завдання підприємства, популярність імені для користувачів, представленість його в Інтернеті та спосіб керування зоною ***DNS*** Інтернет-домену. Як вже сказано, суфікс є необхідною складовою частиною імені домену. Оскільки домени ***Active Directory*** іменуються так само, як домени Інтернету, то виникають дві можливості:

- суфікс, що збігається з іменем Інтернет-домену верхнього рівня ***(com, org, ru, ua).*** Якщо в підприємства вже є зареєстроване доменне ім'я ***company.com***, то воно може використати суфікс ***com*** і для домена ***Active Directory***. Якщо підприємство в Інтернеті ще не представлено, то згодом воно зможе використати для представництва готове ім'я домена ***AD*** за умови, що не виникне конфлікту із чужим раніше зареєстрованим доменним ім'ям;
- суфікс, який не можна використати в Інтернеті. Якщо підприємство не збирається реєструвати свій домен ***AD*** як Інтернет-домен, то як суфікс можна використати що завгодно, наприклад, ***local***. У кожного варіанта є свої плюси й мінуси. Все залежить від того, що в конкретному випадку буде вигідне підприємству. Звичайно адміністратори керуються правилом: якщо підприємство має або планує завести Інтернет-представництво ***(company.com)***, то ім'я внутрішнього домена повинне бути іншим, таке, котре неможливо використати в Інтернеті ***(company.local).*** Справа в тому, що підприємство саме керує зоною ***DNS*** свого Інтернет-домена, і таке рішення дозволяє відокремити керування цією зоною від керування зоною ***DNS*** для потреб домену ***Active Directory***.

У ***Windows Server 2016*** існує можливість зміни імені ***Active Directory***. Для цього призначена утиліта ***Domain Rename Tool***, що перебуває на інсталяційному компакт-диску; її також можна скачати із сайту компанії ***Microsoft.***

Групові політики (Group Policy) — це частина технології ***IntelliMirror***, що з'явилася із приходом системи ***Windows 2000.*** Оснастка ***Групові політики*** продовжує ідеї ***Диспетчера облікових записів*** у системі ***Windows NT 4.0***, але в порівнянні з ним більш функціональна й простіша в розумінні й керуванні. ***Групова політика*** є саме тим засобом, який призначений для спрощення керування комп'ютерами користувачів.

Засіб ***Групова політика*** є в кожному комп'ютері із системою ***Windows 2000*** і вище, і на локальному комп'ютері його можна запустити двома способами:

- запуском порожньої консолі ***mmc*** і додаванням модуля оснащення з назвою ***Групова політика***;
- введенням команди ***gpedit.msc*** у командному рядку або у вікні ***Пуск→Виконати***.

Політики (усього їх більше 700) згруповані у дві гілки: ***Конфігурація комп'ютерів*** і ***Конфігурація користувачів***. Усі політики, задані в частині ***Конфігурація комп'ютера***, застосовуються до комп'ютера незалежно від того, який користувач за ним працює. Політики, задані в частині ***Конфігурація користувача***, застосовуються до облікового запису користувача незалежно від того, за яким комп'ютером він зареєстрований. Деякі політики присутні в обох гілках, інші — тільки в одній.

Майже кожна політика може перебувати в одному із трьох станів:

- не задано (не визначено);
- включено;
- відключено.

Набір станів всіх політик становить ***Об'єкт групової політики (Group Policy Object).*** Його можна застосувати в домені ***Active Directory*** на певному рівні: на рівні всього домену або окремого контейнера.

Якщо створите об'єкт групової політики й застосуєте його на рівні домену, то політики, що входять в гілку ***Конфігурація комп'ютера***, вплинуть на всі комп'ютери в домені, а політики в гілці ***Конфігурація користувача*** вплинуть на всіх користувачів домену. За замовчуванням такий об'єкт уже створений. Він називається ***Default Domain Policy (доменна політика за замовчуванням).*** Його основним призначенням є настроювання параметрів облікових записів користувачів домену.

Якщо створите інший об'єкт групової політики й застосуєте його на рівні ***Domain Controllers*** (який містить тільки облікові записи контролерів домену), то політики з гілки ***Конфігурація комп'ютера*** будуть застосовані тільки до облікових записів комп'ютерів у даній організаційній одиниці (тобто тільки на контролерах домена), а політики в гілці ***Конфігурація користувача*** не будуть застосовані взагалі, оскільки в контейнері ***Domain Controllers*** немає ніяких облікових записів користувачів. За замовчуванням такий об'єкт уже створений, і називається він ***Default Domain Controllers Policy.*** Він призначений для початкового настроювання контролера домена. В ієрархічній структурі домену ***Active Directory*** має місце таке поняття як ***спадковість***. Це означає, що політики з

об'єкта, застосовані до вищого в ієрархії контейнера, автоматично застосовуються й до підлеглих контейнерів, якщо включено режим спадкування. Особливе положення займають локальні об'єкти групової політики. Вони застосовуються тільки до локального комп'ютера й локальних користувачів.

Якщо знищити об'єкт групової політики, то всі політики повернуться в стан за замовчуванням. Те ж відбудеться у випадку переміщення облікового запису користувача в ієрархії ***Active Directory*** на інше місце, де на нього ніякий об'єкт групової політики не діє.

Хід роботи

1. ***Пуск (Start)*** → **Диспетчер серверів.**

Додамо нашому серверу домен. Для цього скористаємося вкладкою **«Add roles and features»** та оберемо **«Active Directory Domain Services»**(рисунок 5.1)**.**

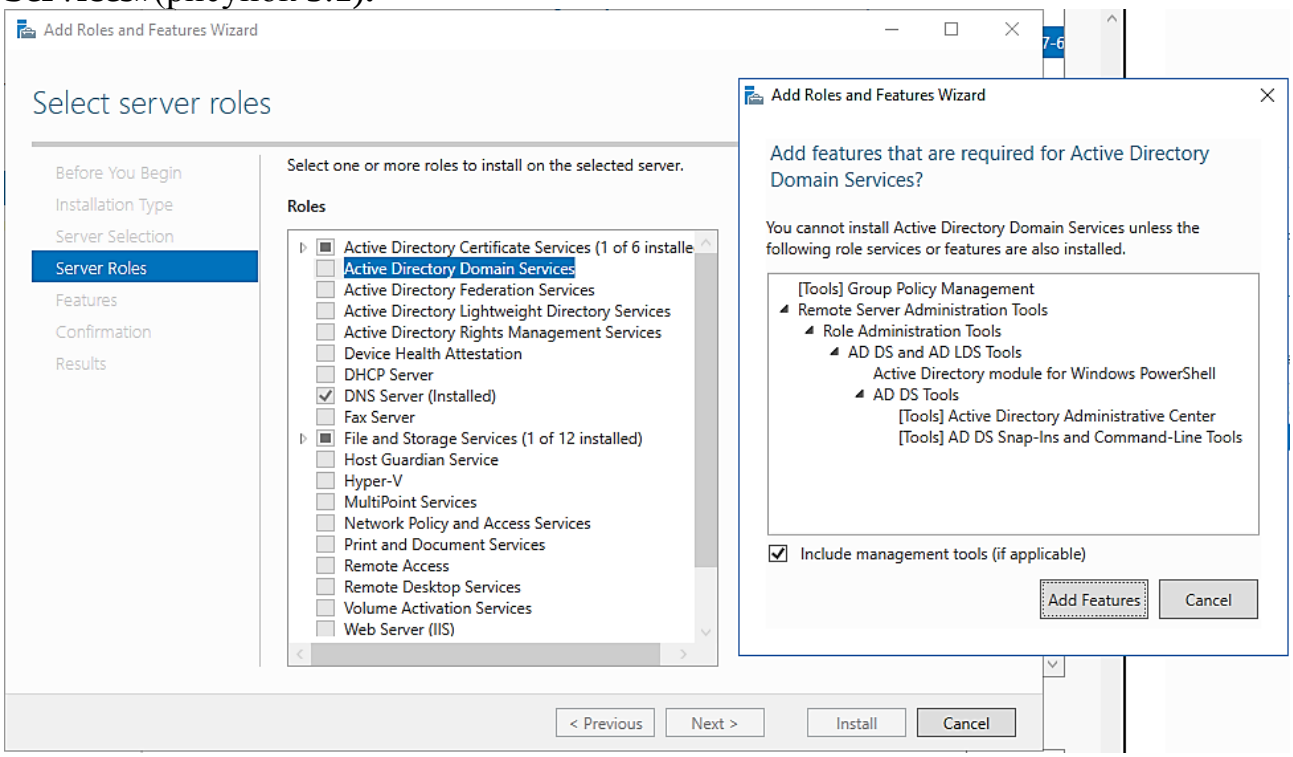

Рисунок 5.1 – Встановлення Active Directory Domain Services

2. Прочитайте відомості, наведені в діалоговому вікні ***Сумісність із операційними системами***, проаналізуйте ці дані й натисніть кнопку ***Далі***. У діалоговому вікні ***Тип контролера домену*** залишіть перемикач у положенні ***Контролер домена в новому домені*** й натисніть кнопку ***Далі*** (рисунок 5.1). У діалоговому вікні ***Створити новий домен*** залишіть перемикач у положенні ***Новий домен у новому лісі*** й натисніть кнопку ***Далі***.

3. У діалоговому вікні ***Нове ім'я*** домену введіть у поле ***Повне DNS-ім'я нового домена***, створеного в попередній роботі (див. таблицю 5.1) й натисніть кнопку ***Далі***. У діалоговому вікні ***NetBIOS–ім'я домену*** залишіть ім'я за замовчуванням і продовжіть натисканням кнопки ***Далі***. У діалоговому вікні

Папки бази даних і журналів залиште запропонований шлях ***C:\WINDOWS\NTDS*** для бази даних й ***C:\WINDOWS\NTDS*** для журналу. Потім натисніть ***Далі***.

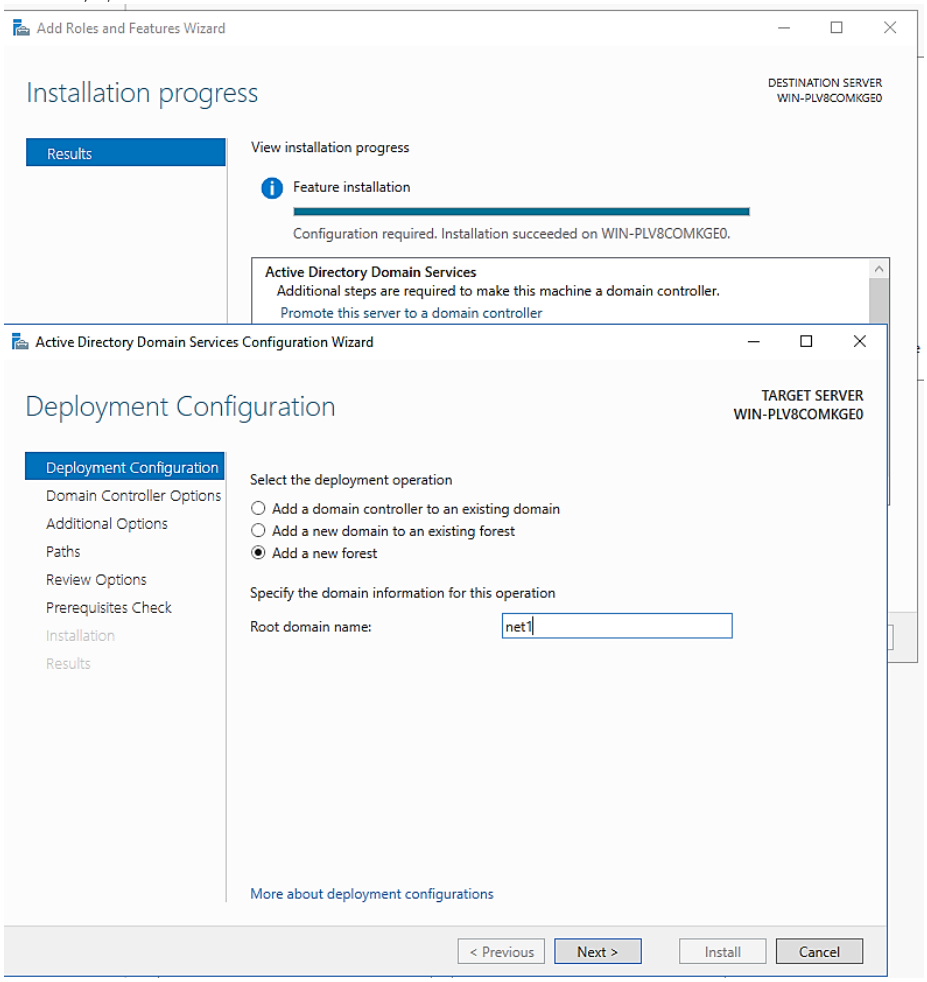

Рисунок 5.2 – Введення DNS-ім'я нового домена

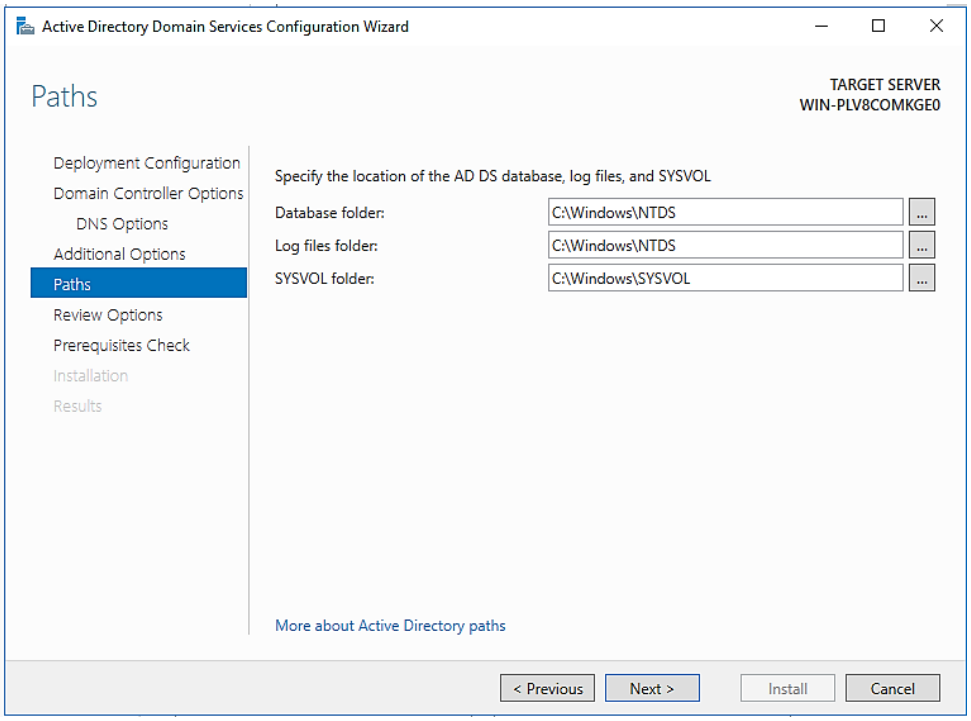

Рисунок 5.3 – Папки бази даних і журналів

4. У діалоговому вікні ***Загальний доступ до системного тому*** залишіть запропонований шлях ***C:\WINDOWS\SYSVOL*** і натисніть ***Далі***. Папку ***SYSVOL*** не можна перемістити надалі. Необхідно, однак, забезпечити, щоб на диску, на якому повинне бути здійснена встановлення, було достатньо вільного місця. Як бачите, ця папка містить об'єкти групових політик, через які вона займає багато місця, і якщо на диску місця недостатньо, то це викличе проблеми з функціональністю домену.

5. Тепер сервер зробить пошук зони ***DNS*** за іменем, що відповідає заданому імені домену. Якщо зона буде знайдена, відобразиться повідомлення про успішно проведену діагностику. Якщо ні — система запропонує її автоматичне встановлення та конфігурування. Прочитавши інформацію, натисніть кнопку ***Далі***.

6. У діалоговому вікні ***Пароль адміністратора для режиму відновлення*** задайте в полі ***Пароль режиму відновлення*** та у полі ***Підтвердження пароля*** пароль, що будете використовувати при відновленні бази даних ***Active Directory***. Потім натисніть кнопку ***Далі***.

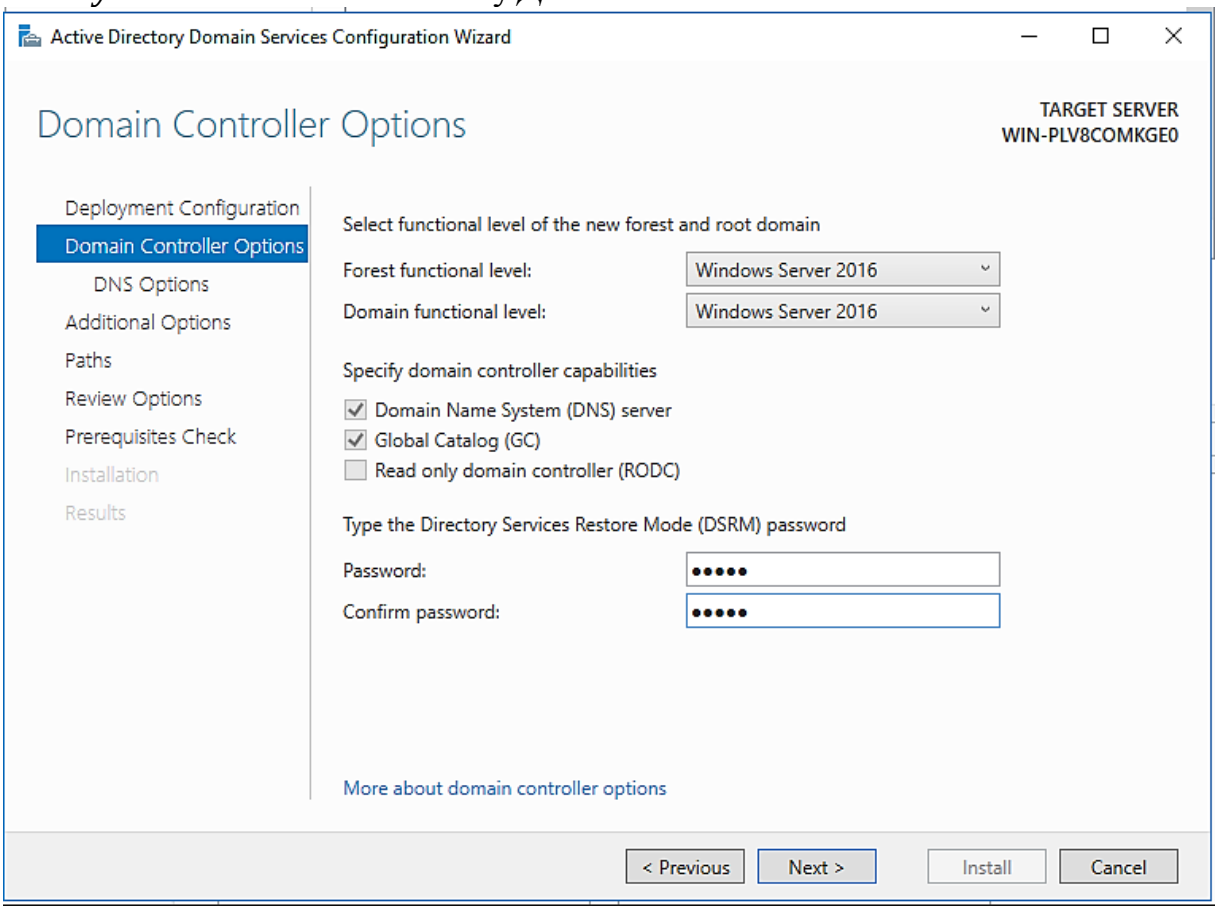

Рисунок 5.4 – Пароль режиму відновлення

7. У діалоговому вікні ***Підсумковий результат*** перевірте коректність настроювання всіх параметрів домену ***Active Directory***. У випадку виявлення яких-небудь помилок натисканням на кнопку ***Назад*** поверніться до діалогового вікна й виправте необхідні параметри. Потім натисканням кнопки ***Далі*** запустіть подальший процес встановлення контролера домену.

Після закінчення роботи ***Майстра встановлення служби Active Directory*** потрібно перезавантажити комп'ютер.

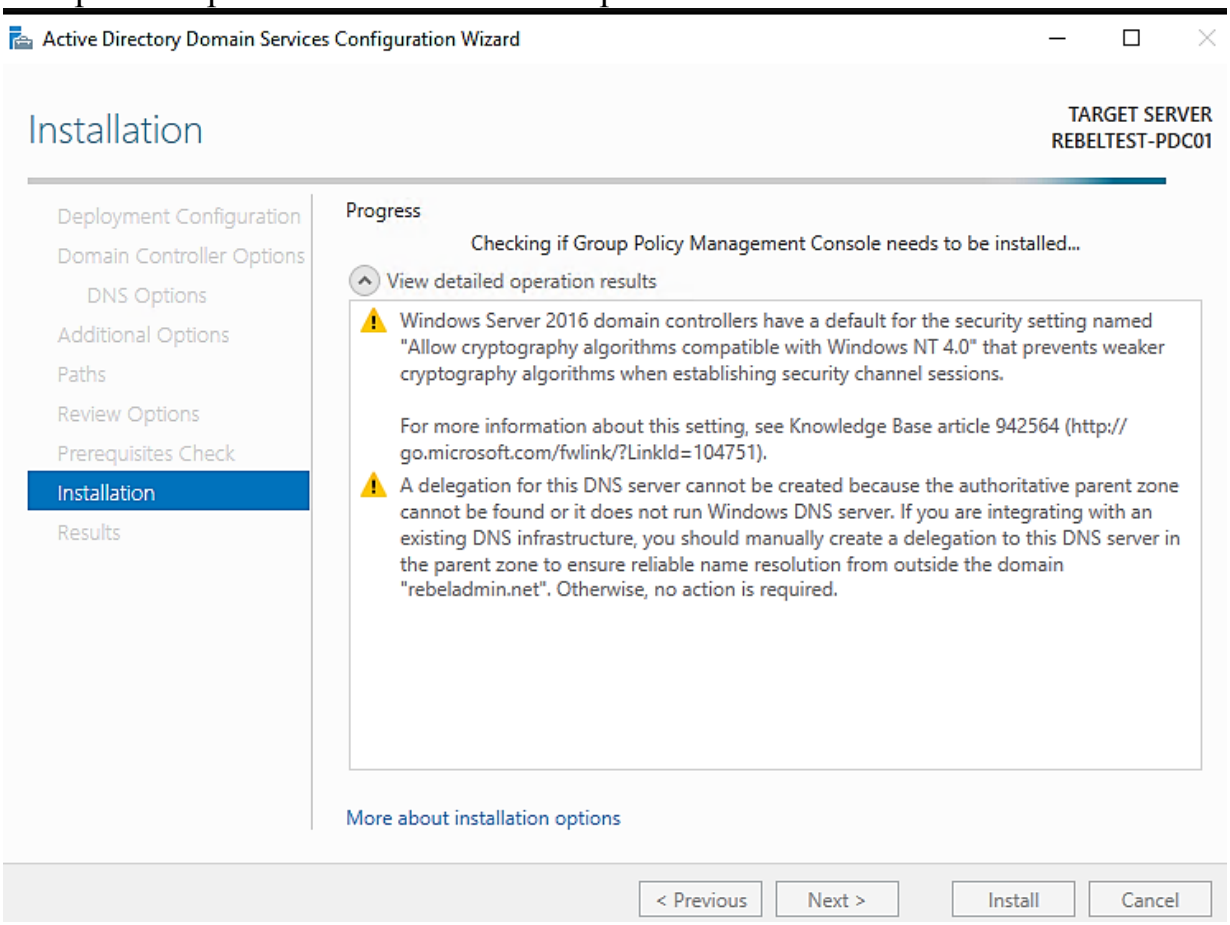

Рисунок 5.5 – Процес інсталяції

8. Після встановлення проведіть перевірку правильності встановлення контролера домену. Результати перевірки внесіть у звіт до лабораторної роботи.

9. Створіть об'єкт групової політики ***OU Information Services1*** і назвіть його ***IS Admin Template Policy.*** Для цього виконайте наступні дії: Зареєструйтеся як користувач ***Administrator*** з паролем ***password***, потім відкрийте утиліту ***Active Directory Users and Computers*** з меню ***Administrative Tools.*** У структурі свого домену MyUnits створіть підрозділ організації ***OU Information Services1.*** Також у цьому підрозділі створіть ще один підрозділ та назвіть його ***«IS Admin Template Policy»*** (без лапок) і натисніть ***Enter.***

10. Створіть об'єкт групової політики для ***OU Customer Support1.*** Назвіть його ***CS Admin Template Policy.*** Для цього виконайте наступні дії: виберіть підрозділ організації ***OU Customer Support1***, відкрийте вікно. Створіть користувача та введіть ***«ISAdmin1»*** (без лапок) і натисніть ***Enter***.

12. Призначте користувачеві ***ISAdmin1*** дозвіл (***permissions***) на читання (***Read***) та запис (***Write***) властивостей об'єкта ***OU Information Services1.***

13. Встановіть обмеження для об'єкта групової політики підрозділу ***Customer Support1.***

- Забороніть зміну пароля;
- Забороніть використання ***Control Panel***.

Таблиця 5.1 – Варіанти завдання

№ варіанту	Ім'я зони	Пароль режиму відновлення
1	net1.local	net1ad
2	net2.local	net2ad
3	net3.local	net3ad
4	net4.local	net4ad
5	net5.local	net5ad
6	net6.local	net6ad
7	net7.local	net7ad
8	net8.local	net8ad
9	net9.local	net9ad
10	net10.local	net10ad

Звіт повинен включати:

1. Тему, мету і порядок роботи.
2. Опис виконання усіх дій.
3. Висновки.

Контрольні питання:

1. Що собою представляє ***Active Directory***?
2. В яких випадках виникає необхідність створення ще одного домену?
3. Які типи суфіксів імені домену існують?
4. Яка утиліта дозволяє змінити ім'я ***Active Directory*** в ***Windows Server 2016***?
5. Як можна запустити засіб ***Групова політика***?
6. Що відбудеться при видаленні об'єкта групової політики?
7. Як встановити обмеження для об’єктів групової політики?

ЛАБОРАТОРНА РОБОТА №6

Тема: «Створення й використання консолі, аналіз та настроювання безпеки».
Мета: навчитися використовувати шаблони безпеки, створені за замовчуванням, а також створювати свої власні.

Теоретичні відомості

Протоколи безпеки мережі використовуються для керування й захисту, аутентифікації, авторизації, конфіденційності, цілісності даних і неможливості заперечення авторства (***nonrepudiation***). До основних протоколів безпеки в мережах ***Windows Server 2016*** відносять: ***Kerberos***, новий ***NTLM (New Technology Local Area Network Manager)***, ***IPSec (Internet Protocol Security)*** та їхні підвиди. Їх підтримують інші протоколи мережевої взаємодії, а їхнє застосування регулюється різними параметрами безпеки.

Шаблони безпеки (Security Templates) і ***Аналіз і настроювання безпеки (Security Configuration and Analysis)*** застосовуються для настроювання параметрів протоколів і підсистеми безпеки.

Завдання реалізації захисту сервера в мережах ***Windows*** розбиваються на три підзавдання. По-перше, треба навчитися розуміти, який захист можна вважати якісним. По-друге, треба вміти забезпечувати безпеку ***IT***-інфраструктури компанії за допомогою наявного остаткування. І нарешті, треба подбати про наявність інструментів і методологій для швидкого настроювання захисту й розуміти, як їх використовувати й підтримувати.

Таблиця 6.1 – Протоколи безпеки мережі

Метод	***Ціль***	***Протокол***
Автентифікація (authentication)	Переконатися, що об'єкт є тим, за кого себе видає	***Kerberos*** (***NTLM*** за замовчуванням недоступний, але його можна сконфігурувати для підтримки аутентифікації)
Авторизація (authorization)	Визначити операції в мережі, дозволені об'єкту, що пройшов аутентифікацію	***Kerberos*** й ***NTLM***
Конфіденційність (confidentiality)	Не допустити компрометації даних	Компоненти шифрування ***Kerberos***, ***NTLM*** й ***IPSec*** (для захисту передачі даних, але не для цілей аутентифікації)
Цілісність (integrity)	Переконатися, що отримано саме ті дані, які були відправлені джерелом	Компоненти ***Kerberos***, ***NTLM*** й ***IPSec***
Неможливість заперечення авторства (nonrepudiation)	Точно визначити, хто відправив і хто прийняв дані	***Kerberos*** й ***IPSec***

Без сумніву, найважливіші політики безпеки визначаються керівництвом, а наведений матеріал дозволить на основі цих політик визначати конкретні параметри безпеки. У минулому при визначенні політик безпеки доводилося застосовувати безліч інструментів і вносити низькорівневі корективи до реєстру. Сьогодні шаблони безпеки й можливість їхнього глобального застосування за допомогою групової політики дозволяють вирішити третє завдання: швидко розгорнути політики безпеки в масштабі підприємства й забезпечити їхню підтримку.

Вкладка ***Шаблони безпеки (Security Templates)*** є однією зі стандартних ***MMC***-консолей. За замовчуванням в ній присутній певний набір шаблонів, параметри яких можна визначати, крім того, можна додавати інші шаблони.

До рекомендованих методів використання шаблонів відносять:

- визначення базового рівня захисту для кожної з ролей комп'ютерів. ***Ролі*** — це функції, що виконуються комп'ютерами, наприклад, контролери домену, файлові сервери й сервери друку, поштові сервери, сервери баз даних, сервери мережних служб (***DHCP***, ***DNS***, ***WINS*** й ін.), ***Web***-сервери, сервери віддаленого доступу тощо;
- визначення принципів безпеки для основних серверних ролей. Загальна для всіх принципів конфігурація захисту звичайно реалізується у вигляді основного (***master***) рівня захисту. Характерні для окремих ролей деталі реалізуються у вигляді додаткових рівнів. У типовій мережі ***Windows Server 2016*** звичайно визначаються два основних рівні: для контролера домену й всіх інших комп'ютерів;
- реалізація основного й додаткового рівнів у шаблонах безпеки;
- застосування основних шаблонів до всіх та додаткових шаблонів — до конкретних комп'ютерів за допомогою інструментів розгортання. Є кілька способів розгортання шаблонів безпеки, у тому числі командні файли й групова політика.

Створення та зміна шаблонів ніяк не впливає на безпеку, поки ви їх не застосуєте. Для застосування шаблону на локальній машині звичайно використовують вкладку ***Аналіз і настроювання безпеки (Security Configuration and Analysis).*** Вона також дозволяє порівнювати параметри будь-якого шаблону з параметрами, що діють у цей час на комп'ютері. Користь від цього величезна. Після завершення аналізу розходження між діючою реалізацією безпеки й обраним шаблоном відзначаються в інтерфейсі користувача червоним хрестом (***x***). Таке порівняння наочно показує, що відбудеться у випадку застосування шаблону.

Але ще корисніша можливість моніторингу безпеки комп'ютера шляхом періодичного порівняння конфігурації безпеки з базовим шаблоном. Це дозволяє виявити невідповідності поточних параметрів безпеки базовому шаблону, а також вивчити й повернути систему у вихідний стан.

Застосовуючи додаткові шаблони, треба вирішити, чи варто очищувати базу даних. При очищенні бази даних застосовуються тільки параметри з

нового шаблону. Але якщо до цього були застосовані параметри старого шаблона, його видалення з бази не спричиняє скасування його параметрів.

Якщо база не очищується, додавання нового шаблона означає наступне:

- якщо параметр не визначений у новому шаблоні, але визначений у старому, його значення залишається заданим у відповідності зі старим шаблоном;
- якщо параметр визначений у новому шаблоні й не визначений у старому, його значення змінюється відповідно до нового шаблону;
- якщо параметр визначений як у новому, так і старому шаблонах, значення задається у відповідності з новим шаблоном.

Одна з найважливіших концепцій розробки й реалізації політики безпеки — принцип найменших привілеїв, тобто жоден зі співробітників й користувачів інформаційної системи не повинен мати більше привілеїв, ніж потрібно йому для виконання роботи. Цей принцип позбавляє користувача привілеїв та прав доступу при звільненні або зміні роботи усередині компанії. Те ж справедливе й для всіх гостей організації або будь-яких її трудових ресурсів — громадськості, контрактників, тимчасових працівників, представників компаній-партнерів тощо.

Ніхто, включаючи системних адміністраторів і співробітників служби ***IT***, не повинен мати більше прав доступу, ніж необхідно для роботи. Існує багато способів реалізації цього принципу, причому їх умовно розбивають на дві категорії: реалізовані за допомогою шаблонів безпеки й інших механізмів.

Хід роботи

1. Створіть консоль, що дозволить переглядати, налаштовувати або копіювати шаблони безпеки, додавати нові папки для зберігання шаблонів, а також застосовувати шаблони до комп'ютера. Робота із шаблонами в консолі ніяк не вплине на безпеку комп'ютера. Для початку створіть консоль ***Аналіз і настроювання безпеки.*** Для цього виконайте наступні дії: запустіть команду ***mmc***. Виберіть у меню ***Файл (File) Додати або видалити оснащення (Add/Remove Snap-In).*** В однойменному вікні клацніть кнопку ***Додати (Add)***.

2. У вікні ***Додати ізольовану оснастку (Add Standalone Snap-In)*** оберіть ***Шаблони безпеки (Security Templates)*** і клацніть кнопку ***Додати (Add)*** (рисунок 7.1). Оберіть оснастку ***Аналіз і настроювання безпеки (Security Configuration and Analysis),*** клацніть ***Додати***, а потім ***Закрити (Close).*** Клацніть ***ОК***, щоб додати обрані оснастки в консоль. Збережіть консоль, обравши в меню ***Консоль*** пункт ***Зберегти як (Save As).*** У полі імені файлу введіть ***Security Configuration Management*** і клацніть ***Зберегти (Save)*** (рисунок 6.1)**.**

3. Підготуйте місце для нестандартних шаблонів безпеки й додавання їх в ***Консоль***. Для цього у вікні ***Провідника*** створіть нову папку з ім'ям ***Custom Templates***. Відкрийте ***консоль Security Configuration Management.*** Клацніть ***Шаблони безпеки (Security Templates)*** правою кнопкою й виберіть ***новий шлях***

для пошуку шаблонів (New Template Search Path). Виберіть папку ***Custom Templates*** і клацніть ***OK***. У консолі ***Security Configuration Management*** з'явиться нова папка.

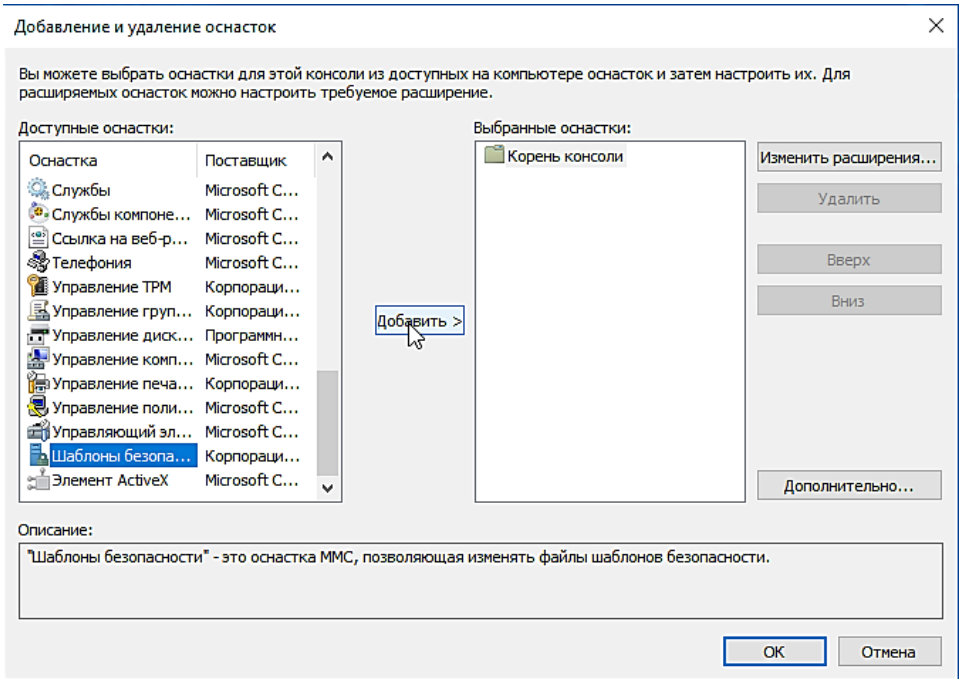

Рисунок 6.1 – Вікно додавання оснастки

Рекомендується ніколи не змінювати шаблони за замовчуванням, а нові (або існуючі, які треба змінити) шаблони розміщувати в окремому місці. При такому способі шаблони за замовчуванням збережуться, а користувальницькі шаблони, які зберігаються окремо, не важко буде при необхідності зберегти в надійному місці (рисунок 6.2).

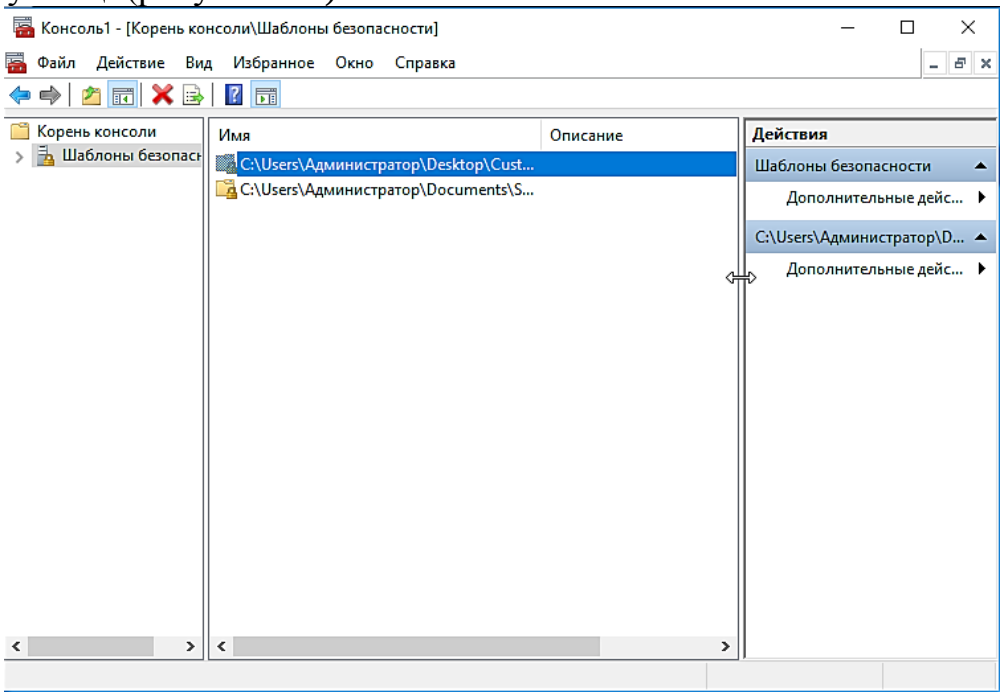

Рисунок 6.2 – Папка для користувальницьких шаблонів

4. У консолі ***Шаблони безпеки (Security Templates)*** виберіть папку ***Custom Templates*** і натиснувши правою кнопкою й виберіть **Створити шаблон** та ***Зберегти як (Save As),***а як ім'я файлу — ***Test1***. Клацніть ***Зберегти (Save).***

5. Розкрийте папку ***Custom Templates*** у консолі ***Security Configuration Management.*** Щоб побачити шаблон ***Test1***, можливо буде необхідно оновити консоль. Розкрийте розділи шаблона ***Test1***. Розкрийте вузол ***Локальні політики (Local Policies)*** і виберіть ***Параметри безпеки (Security Options)*** (рисунок 6.3).

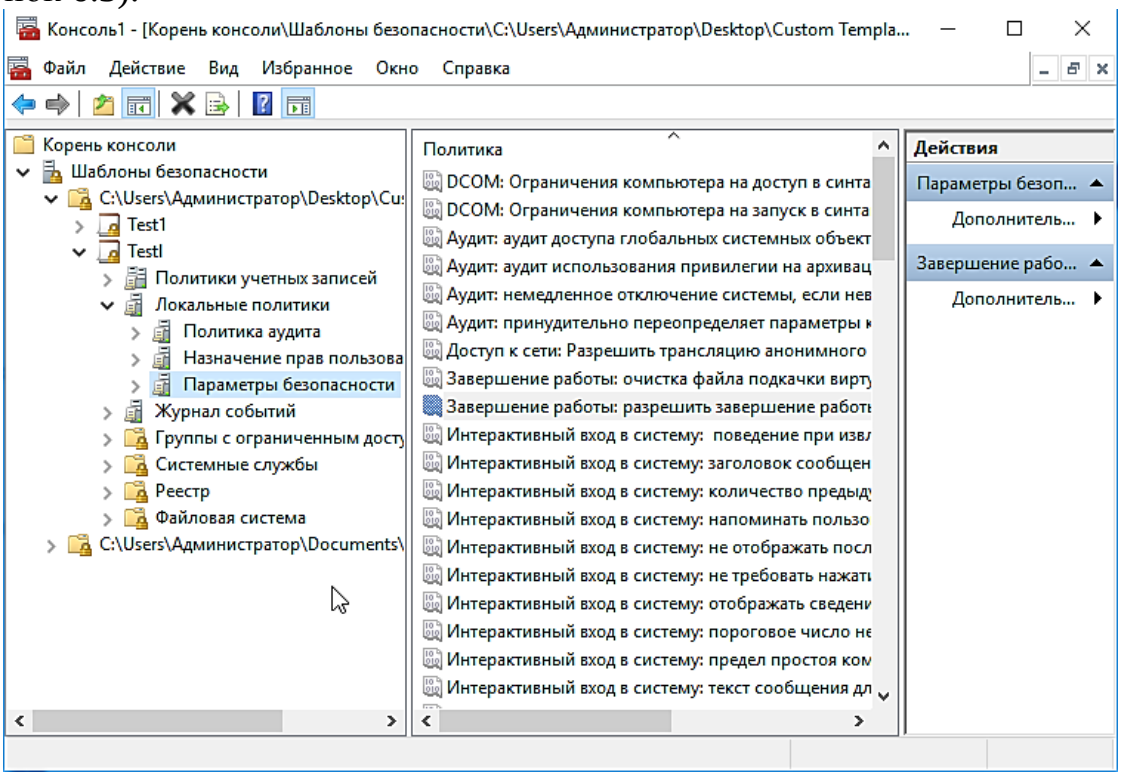

Рисунок 6.3 – Параметри безпеки

6. Знайдіть у правій панелі розділи ***Мережевий доступ (Network Access)*** і ***Мережева безпека (Network Security)*** і вивчіть їхнє значення. Зверніть увагу, що значення політики — ***Не визначений (Not defined).*** Двічі клацніть на політику ***Завершення роботи: дозволити завершення роботи системи без виконання входу в систему (Shutdown: Allow System to Be Shut Down Without Having to Log on).*** Відкриється вікно властивостей політики (рисунок 6.4). Встановіть прапорець ***Визначити наступний параметр політики в шаблоні (Define This Policy Setting in The Template)*** (якщо він ще не встановлений) і відзначте перемикач ***Відключений (Disabled).*** Клацніть ***ОК***. Параметри й методи визначення залежать від параметра. У багатьох політиках треба спочатку встановити прапорець ***Визначити наступний параметр політики в шаблоні*** — лише після цього можна змінювати окремі параметри. Збережіть внесені зміни, клацнувши правою кнопкою на імені шаблона й вибравши в контекстному меню ***Зберегти (Save)*** (рисунок 6.4)**.**

7. У вікні ***Провідника*** перейдіть у папку ***Custom Template***. Двічі клацніть шаблон ***Test1***, щоб відкрити його у вікні ***Блокнот (Notepad).*** Вивчіть розділ

[Registry Values]. Тут змінюють або додають розділи реєстру, на які подіє шаблон у випадку його застосування.

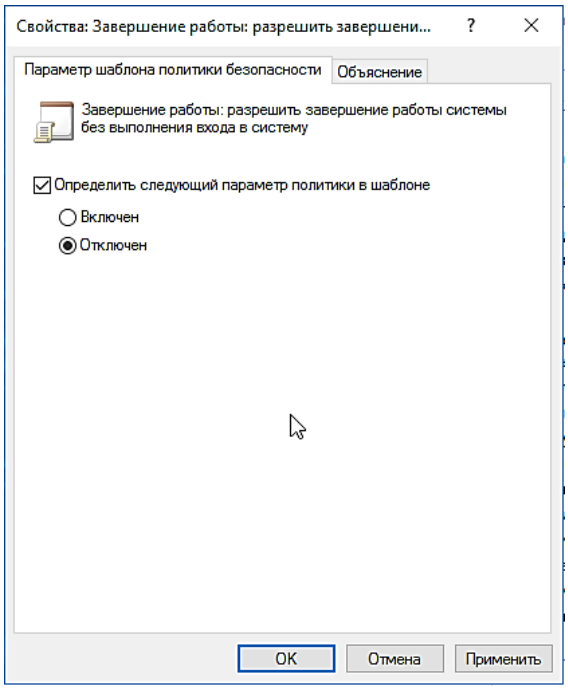

Рисунок 6.4 – Зміна параметрів шаблона

8. Створіть шаблон відкату командою:

secedit /generaterollback /cfg Test1.inf /rbk Test1rollback. inf / log Test1rollback.log

Ця команда створює шаблон, що у випадку неполадок поверне параметри до стану перед застосуванням шаблона ***Test1.inf.*** Спочатку створюється шаблон ***Testlrollback.inf,*** а потім застосовується ***Test1.inf.*** Відкат значень неможливий для параметрів безпеки файлів та реєстру, тобто у випадку застосування «зворотнього» шаблона будь-які зміни, внесені шаблоном у ці дозволи, не скасуються (рисунок 6.5).

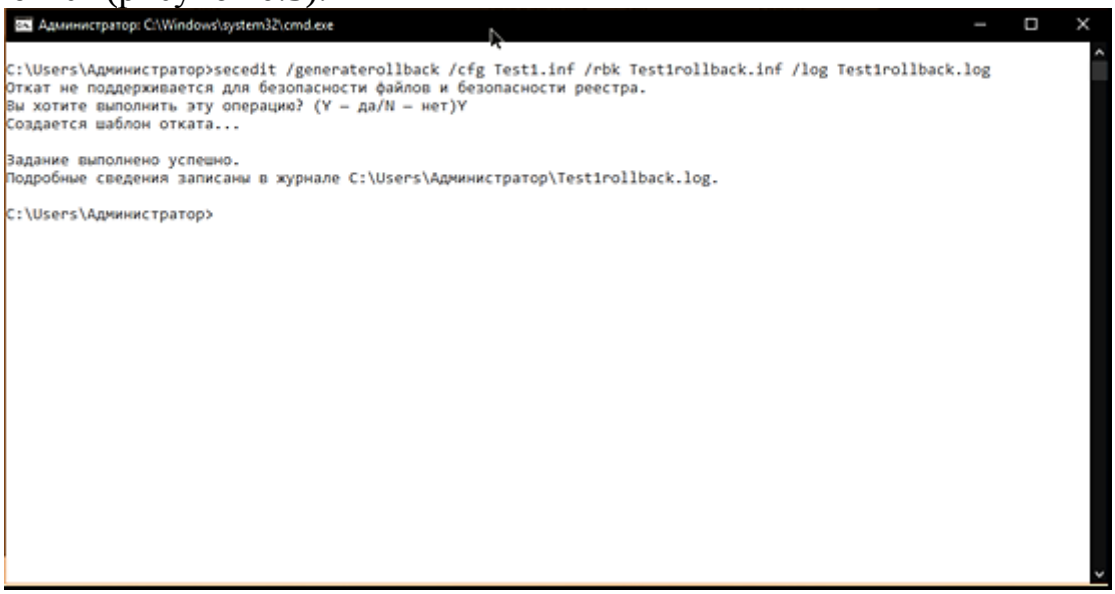

Рисунок 6.5 – Створення шаблону відкату

Звіт повинен включати:

1. Тему, мету і порядок роботи.
2. Опис виконання усіх дій.
3. Висновки.

Контрольні питання:

1. Для чого використовуються протоколи безпеки мережі?
2. На які підзавдання підрозділяється завдання реалізації захисту сервера?
3. Які методи використання шаблонів безпеки рекомендуються?
4. Яка оснастка звичайно використовується для застосування шаблона на локальному комп'ютері?
5. Треба застосувати нові параметри реєстру на всіх серверах мережі. Як виконати завдання з найменшими зусиллями?
6. Які з наведених далі параметрів можна застосувати за допомогою оснастки ***Аналіз і настроювання безпеки (Security Configuration and Analysis)*** і шаблона безпеки? Виберіть всі підходящі варіанти:
   а) пароль повинен бути не менше 15 символів;
   б) групі ***Бухгалтери (Accountants)*** треба заборонити доступ до цього комп'ютера за мережою;
   в) будь-яка мережна взаємодія комп'ютерів ***Computerl*** й ***Computer2*** повинна виконуватися з використанням ***IPSec***;
   г) необхідно встановити наступні кореневі дозволи для файлів: рівень доступу ***Повний доступ (Full Control);*** група — ***Всі (Everyone).***
7. З чого необхідно почати відновлення «статуса-кво» після застосування шаблона безпеки, після якого файловий сервер став недоступним за мережою для всіх користувачів? Виберіть найбільш ефективний спосіб:
   а) локально ввійти в систему файлового сервера як ***Адміністратор (Administrator)*** і застосувати кореневий шаблон безпеки;
   б) локально ввійти в систему файлового сервера як ***Адміністратор (Administrator)*** і застосувати шаблон відкату, створений перед застосуванням «некоректного» шаблона безпеки;
   в) виконати віддалений вхід у систему файлового сервера під обліковим записом члена групи ***Адміністратори підприємства (Enterprise Admin)*** і в консолі ***Локальна політика безпеки (Local Security Policy)*** змінити некоректні (на ваш погляд) політики прав користувачів;
   г) виконати віддалений вхід у систему файлового сервера як ***Адміністратор (Administrator)*** і застосувати шаблон відкату, створений на основі шаблона безпеки.

ЛАБОРАТОРНА РОБОТА №7

Тема: «Встановлення операційної системи Windows 7 з Windows Server 2016».
Мета: навчитися встановлювати операційну систему з локальної мережі.

Хід роботи

На фізичній, чи віртуальній машині у якості пріоритетного пристрою при завантаженні машини обрати мережевий адаптер. У випадку виконанні в VirtualBox, чи будь-якій іншій віртуальній машині також необхідно обрати мережеву карту комп'ютера, чи віртуальний адаптер хоста, як зображено на рисунках 7.1 та 7.2.

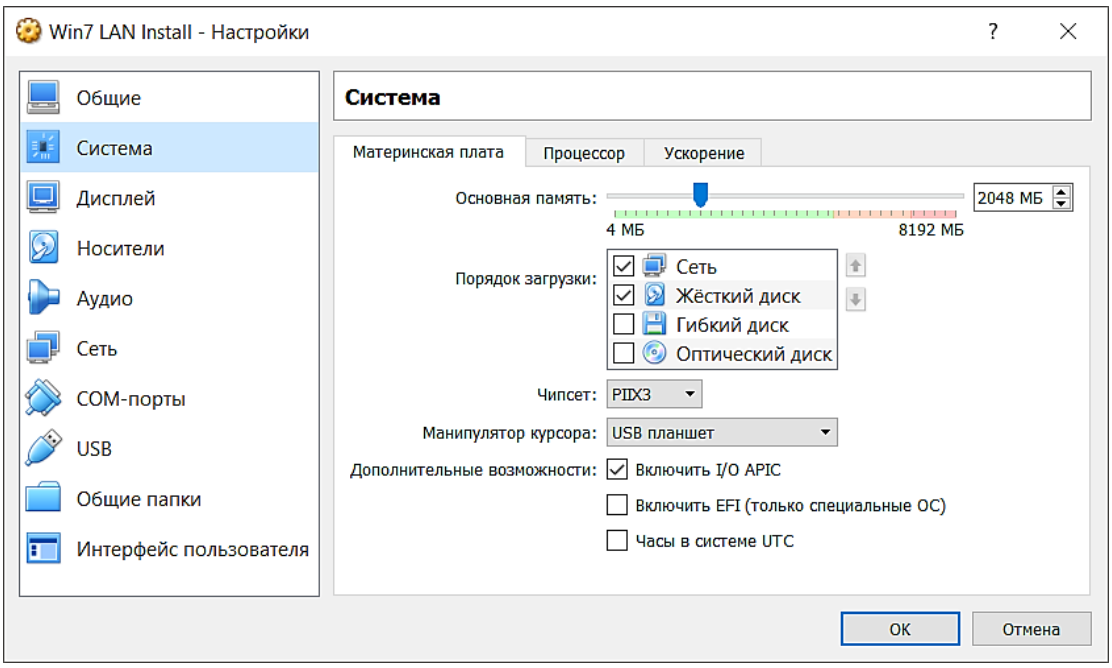

Рисунок 7.1 – Пріоритетний пристрій завантаження

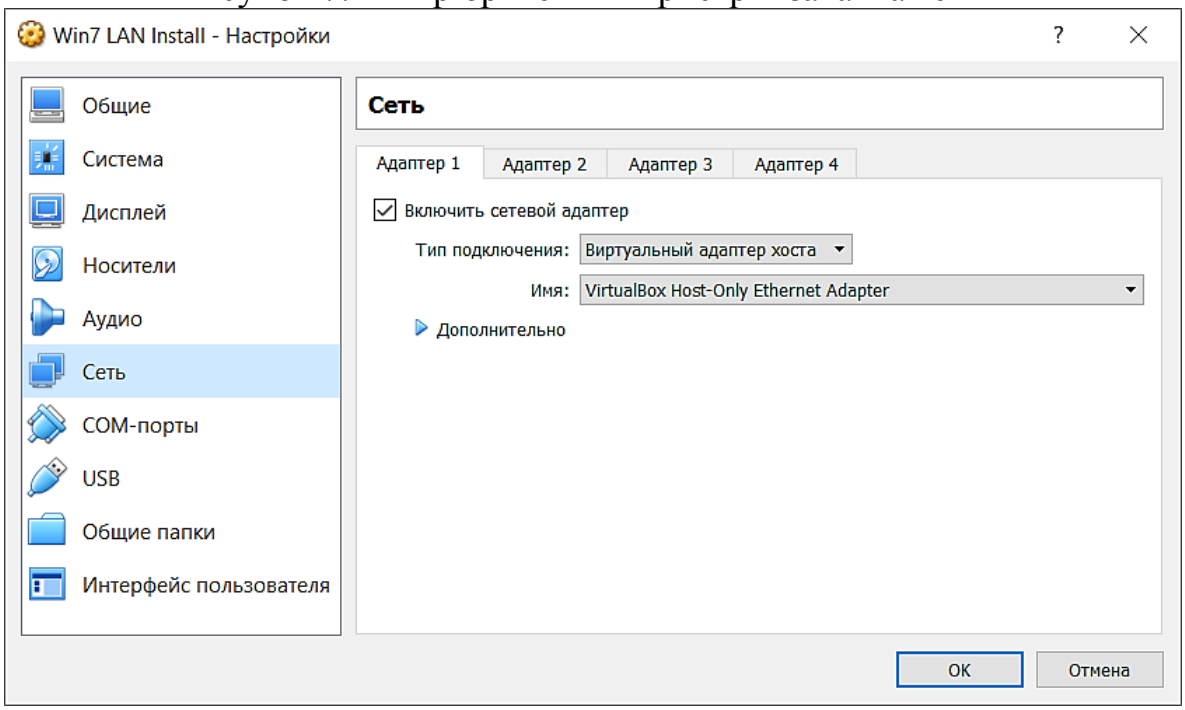

Рисунок 7.2 – Вибір мережевого адаптеру

Встановити TFTP сервер через Майстер додавання ролей та компонентів. Необхідний компонент – «Службы развёртывания Windows», зображений на рисунку 7.3.

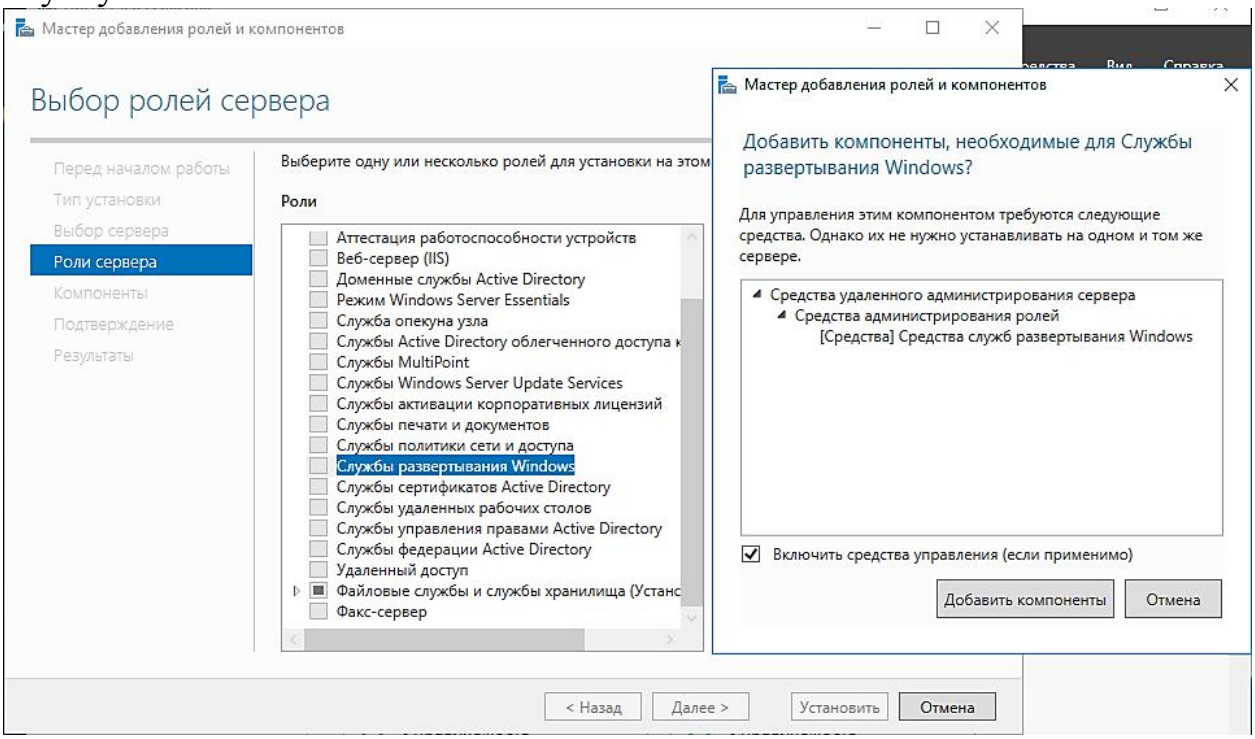

Рисунок 7.3 – Встановлення необхідного компоненту

Після завершення установки ролі необхідно створити каталог, який буде кореневим каталогом для TFTP сервера, наприклад **C: \ tftp**. Потім за допомогою редактора реєстру в гілці **HKLM \ SYSTEM \ CurrentControlSet \ services \ WDSServer \ Providers \ WDSTFTP** створимо новий строковий (String) параметр з ім'ям RootFolder, і значенням, що містить шлях до кореневого каталогу TFTP, створеному раніше. Виконання операції зображено на рисунку 7.4.

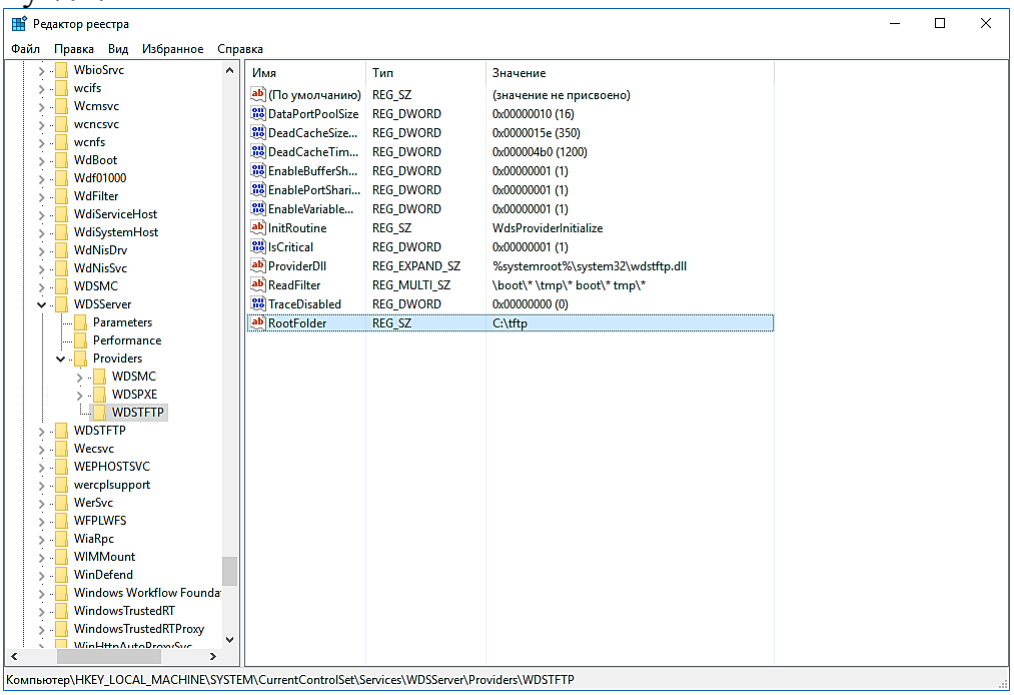

Рисунок 7.4 – Редагування реєстру

Запустимо службу WDS за допомогою команди **WDSUTIL / Start-TransportServer**. Результат успішного виконання команди зображене на рисунку 7.5.

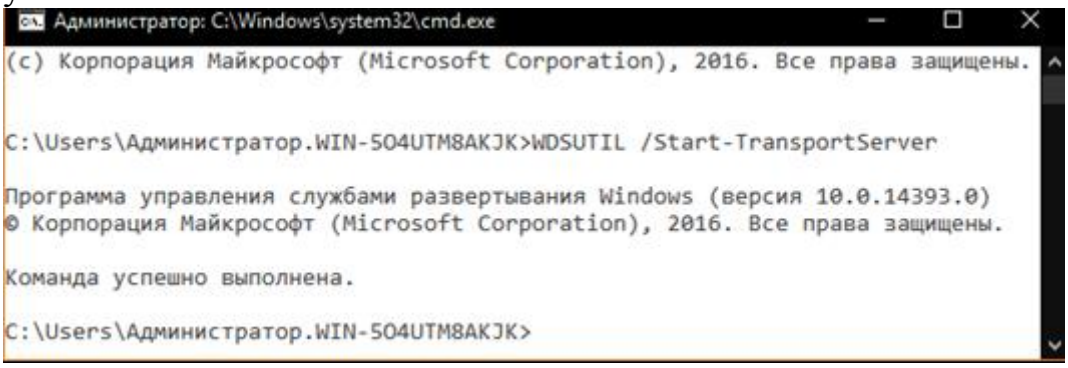

Рисунок 7.5 – Запуск служби WDS

При встановленому TFTP клієнті перевірити сервер можна за допомогою команди **tftp –i localhost GET tmp\test.txt C:\test.txt** попередньо створивши відповідний файл у каталозі **tftp**.

У результаті правильної роботи серверу буде видано повідомлення, зображене на рисунку 7.6.

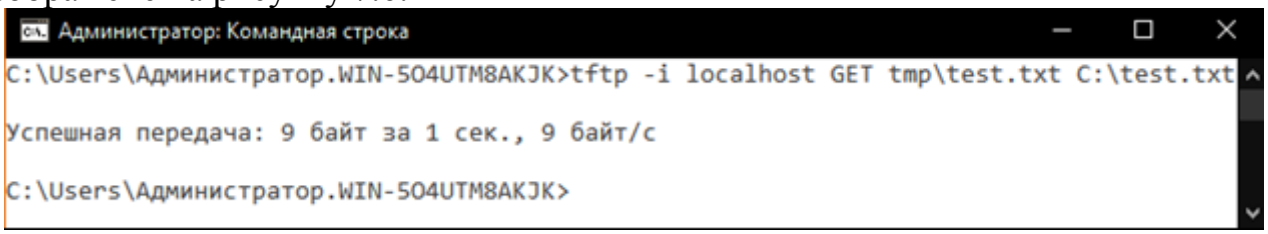

Рисунок 7.6 – Правильна робота TFTP-серверу

Тепер необхідно скачати та встановити пакет Windows AIK. У головному меню «Пуск» знаходимо Microsoft Windows AIK і запускаємо «Командний рядок коштів розгортання» - відкриється консоль. В консолі засобів розгортання вводимо наступні команди: **copype.cmd x86 C:\winpe** та **imagex /mountrw winpe.wim 1 mount**. Результат їх виконання зображено на рисунку7.7.

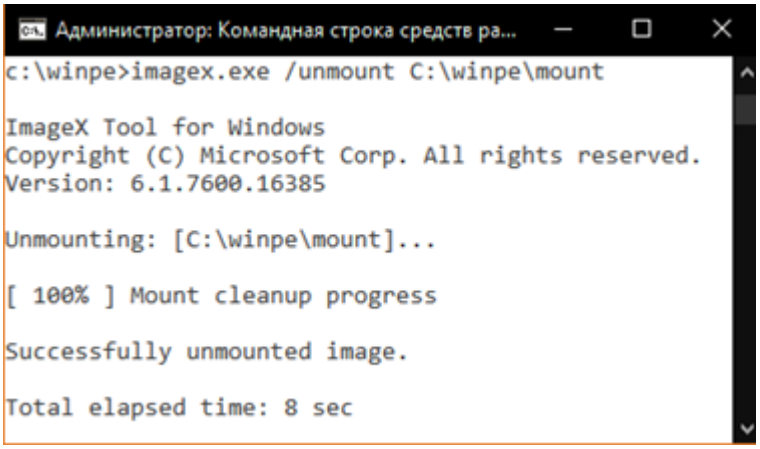

Рисунок 7.7 – Монтування системи

Далі, щоб позбутися від необхідності вручну підключати мережевий диск і форматувати запуск виконуваного додатка, необхідно відкоригувати командний файл **startnet.cmd**, розташований в каталозі **C: \ winpe \ mount \ windows \ system32**. Структура файлу повинна бути такою:

wpeinit
net use y: \\192.168.1.1\seven /user:install install
if exist y:\sources\setup.exe (
y:
cd \sources
setup.exe
)

У даному випадку мається на увазі, що IP-адреса комп'ютера, з якого будуть завантажуватися файли з мережі, має значення 192.168.1.1, якщо він відрізняється від прикладу, то впишіть конкретну адресу. Підключення до комп'ютера з боку другого ПК, на який і виробляється установка, буде відбуватися на правах користувача **install** з паролем **install**, тому необхідно заздалегідь створити такого користувача, наприклад скориставшись командою: **net user install install /add /passwordchg:no**

Тепер необхідно демонтувати створений образ. Виконуємо в консолі наступну команду: **imagex.exe /unmount /commit mount**.

Створюємо на комп'ютері папку, з якої в подальшому будуть завантажуватися з мережі файли дистрибутива, наприклад **C: \ tftp**, в ній створюємо ще один каталог - **boot (C: \ tftp \ boot)**, у ньому будуть розташовуватися завантажувальні файли.

Копіюємо в папку **C: \ tftp** каталог sources з наявного дистрибутива Windows 7.

У консолі виконуємо кілька команд, за допомогою яких заповнюємо каталог boot і робимо можливим виконання завантаження файлів з мережі:

imagex.exe /mount C:\winpe\winpe.wim 1 C:\winpe\mount.
xcopy /ey C:\winpe\mount\windows\boot\pxe C:\tftp
xcopy /iy C:\winpe\mount\windows\boot\fonts C:\tftp\boot\fonts
copy /y C:\winpe\ISO\boot\boot.sdi C:\tftp\boot
imagex.exe /unmount C:\winpe\mount

Копіюємо недавно створений образ winpe.wim в папку C: \ tftp \ boot, наприклад скориставшись командою: **copy /y C:\winpe\winpe.wim C:\tftp\boot**
Відкриваємо загальний доступ до папки C: \ upload для ВСІХ користувачів та виконуємо команду: **createbcd.cmd x:\upload\boot**

Звіт повинен включати:

1. Тему, мету і порядок роботи.
2. Опис виконання усіх дій.
3. Висновки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Сёмин И. Как установить Telnet клиента в Windows Server 2012R2 [Електронний ресурс] / Иван Сёмин. – 2015. – Режим доступу до ресурсу: http://pyatilistnik.org/kak-ustanovit-telnet-klienta-v-windows-server-2012r2/.
2. Установка доменных служб Active Directory (уровень 100) [Електронний ресурс] // Microsoft. – 2017. – Режим доступу до ресурсу: https://docs.microsoft.com/ru-ru/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-.
3. Установка нового Active Directory леса Windows Server 2012 (уровень 200) [Електронний ресурс] // Microsoft. – 2017. – Режим доступу до ресурсу: https://docs.microsoft.com/ru-ru/windows-server/identity/ad-ds/deploy/install-a-new-windows-server-2012-active-directory-forest--level-200-.
4. Пошаговое руководство: настройка DHCP с использованием назначения на основе политики [Електронний ресурс] // Microsoft. – 2017. – Режим доступу до ресурсу: https://technet.microsoft.com/ru-ru/library/hh831538(v=ws.11).aspx.

ДОДАТКОВА ЛІТЕРАТУРА

1. Tanenbaum A. S. Современные операционные системы (Modern Operating Systems) / A. S. Tanenbaum, H. Bos. – СПб: Питер, 2015. – 1120 с. – (Классика Computer Science; 4).
2. Линн С. Администрирование Microsoft Windows Server 2012 / Самара Линн. – СПб: Питер, 2014. – 304 с.
3. Олифер Н.А., Олифер В.Г. Сетевые операционные системы: Учебник для вузов, 2-е изд. СПб.: Питер, 2007. – 672 с.
4. Поляк-Брагинский А.В. Администрирование сети на примерах. / А. В. Поляк-Брагинский – СПб.: БХВ-Петербург, 2005. – 320 с.
5. Таненбаум Э. Операционные системы: разработка и реализация / Э. Таненбаум, А. Вудхалл. – СПб: Питер, 2007. – 704 с. – (Классика Computer Science).

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт

з дисципліни «МЕРЕЖНІ ОПЕРАЦІЙНІ СИСТЕМИ»

(Windows Server 2016)

для студентів спеціальності

123 «Комп’ютерна інженерія»

усіх форм навчання

УКЛАДАЧІ: **Кумченко Юрій Олександрович**

Музика Іван Олегович

Реєстраційний № ___

Підписано до друку _____ 2018 р.

Формат А5

Обсяг 67 стор.

Тираж _____ прим.

Видавничий центр

ДВНЗ «Криворізький національний університет»,

вул. Віталія Матусевича, 11, м. Кривий Ріг